REGLENE FOR IDENTIFIKASJON AV KOMMUNIKASJONSANLEGG I FORHOLD TIL EMK ART. 8

Kandidatnummer: 331

Veileder: Stine Laier Nybø

Leveringsfrist: 25.11.2005

Til sammen 17 867 ord

30.11.2005

Innholdsfortegnelse

1 Innledning

1.1 Bakgrunn for oppgaven og presentasjon av problemstilling

Bakgrunnen for denne oppgaven er den senere tids debatt rundt behovet for regler om identifikasjon av kommunikasjonsanlegg. Debatten har sitt utspring i de kriminelles bruk av mobiltelefoner og annet teknisk kommunikasjonsutstyr som ledd i forberedelsen av kriminelle handlinger. For politiet har det vært et stadig tilbakevendende problem at de ikke alltid har kjent identiteten på telefonene og annet teknisk kommunikasjonsutstyr forbryterne har benyttet seg av. Dette har skapt forsinkelse og vanskeligheter i etterforskningen av kriminelle handlinger, da avlytting i disse tilfellene har vært avskåret. Etter straffeprosessloven kapittel 16 a §§ 216 a og 216 b er det et krav at de kommunikasjonsanlegg som skal avlyttes, identifiseres entydig.[1] Identiteten må inngå som del av begjæringen om kommunikasjonskontroll. Med kommunikasjonsanlegg menes her telefon, telefaks, datamaskin og mobiltelefon. (Se nærmere om dette i 2.1.2.) Eksempel på slik identitet er nummeret til en fasttelefon eller SIM-kortets nummer. (Se nærmere i 1.3.) Der politiet ikke innehar den nødvendige informasjon, er de avskåret fra å få kjennelse på avlytting.

Det er nødvendig å se behovet for de nye reglene i lys av kriminalitetsutviklingen. Det blir i Ot.prp. nr. 60 (2004-2005) lagt til grunn at alvorlig og organisert kriminalitet utgjør en større trussel nå enn for bare noen år siden.[2] Terrortrusselen mot Norge er begrenset, men kan lett endre seg etter forholdene ellers i samfunnet. Dette kommer frem i en rapport

[1] Lov 22. mai 1981 nr. 25 (strpl.)

[2] Ot.prp. nr. 60 (2004-2005) Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet) punkt 3.4 side 24 flg.

utarbeidet av Norsk Utenrikspolitisk Institutt (NUPI) i januar 2005.[3] De kriminelle synes å ha blitt mer profesjonelle og forbrytelsene mer brutale og hensynsløse, samtidig virker planleggingen grundigere og mer organisert. Norge har tradisjonelt vært forsiktig med å ta i bruk inngripende etterforskningsmetoder. Disse metodene bør bare kunne tas i bruk ved bekjempelse av særlig alvorlige forbrytelser. Slik situasjonen også er etter strpl. §§ 216 a og 216 b. I Ot.prp. nr. 60 (2004-2005) side 32 uttales det "[h]ensynet til den enkeltes rettssikkerhet og krav på personvern tilsier at lovgiverne bare bør utvide bruken av tvangsmidler på områder hvor kriminalitet utgjør en alvorlig trussel, og hvor politiet ikke kan bekjempe denne trusselen effektivt med allerede tillatte virkemidler."

Med utgangspunkt i et eventuelt behov for regler for identifikasjon av kommunikasjonsanlegg, ble det 4. juni 2004 sendt ut et høringsbrev. Departementet følger i Ot.prp. nr. 60 (2004-2005) opp de forslag til endringer i straffeprosessloven som ble forslått i høringsbrevet. Endringene ble vedtatt 17. juni dette år, og trådte i kraft 5. august.[4] Reglene er et utslag av kryssende hensyn; hensynet til enkeltindividets personvern og samfunnets ønske om å oppklare kriminalitet.

I det følgende skal de nye reglene for identifikasjon i strpl. §§ 216 a tredje ledd annet punktum og 216 b annet ledd litra c) behandles. Det skal vurderes i hvilken grad reglene er i overensstemmelse med Den europeiske menneskerettskonvensjon (EMK) art. 8 "Retten til respekt for privatliv og familieliv".[5] Fremstillingen baserer seg på lovens ordlyd, forarbeidene og juridisk litteratur. Rettspraksis på området er ikke offentlig, det er derfor ikke mulig å si noe om omfanget av bruken av de norske reglene, og heller ikke hvorvidt

---

[3] Ot.prp. nr. 60 (2004-2005) punkt 3.4.4 side 31

[4] Lov 17. juni 2005 nr. 87 (i kraft 5. august 2005 i følge resolusjon 5. august 2005 nr. 849)

[5] Menneskerettsloven (mnskrl.) av 21. mai 1999 nr. 30 § 2 bestemmer at Den europeiske menneskerettskonvensjonen (EMK) skal gjelde som norsk lov. EMK (Convention for the Protection of Human Rights and Fundamental Freedoms) ble åpnet for undertegning 4. november 1950 og trådte i kraft 3. september 1953.

domstolene legger til grunn andre vurderingstemaer for reglene enn de som fremkommer under.

1.2 Avgrensning av problemstilling

På grunn av oppgavens omfang vil ikke de øvrige former for kommunikasjonskontroll bli behandlet, eksempelvis telefonavlytting i snever forstand og annen form for kontroll etter strpl. § 216 b annet ledd. De ulike vilkår som må være oppfylt for å kunne begjære slik kontroll etter strpl. §§ 216 a og 216 b, vil likevel bli behandlet da de er de samme som for identifisering. Eventuelle begrensinger i folkeretten, eksempelvis hvorvidt diplomatisk immunitet er til hinder for kommunikasjonskontroll, vil ikke bli behandlet. Heller ikke vil FN konvensjonen om sivile og politiske rettigheter art. 17 bli behandlet. Dette fordi artikkelen gir lite vern utover EMK art. 8

Når det gjelder politiets forebyggende og avvergende virksomhet i henhold til politiloven § 17 d og strpl. § 222 d, vil heller ikke dette bli utførlig behandlet.[6] Se 1.7 for kort innføring.

1.3 Kravet til entydig identifikasjon

Alle kommunikasjonsanlegg har en form for identitet. Identiteten kommer til uttrykk på forskjellige måter for de forskjellige former for anlegg. Fasttelefoner identifiseres med telefonnummer, det samme gjelder for telefaks, personsøker og teleks.

For datamaskiner er situasjonen en annen. Alle datamaskiner får utdelt en IP-adresse (Internet Protocol) fra nettleverandør når de kobler seg opp på enten internett eller intranett. Adressen kan spores tilbake til eier av abonnementet. Dette kan likevel være vanskelig i de tilfeller der en får ny IP-adresse hver gang en kobler seg opp på nettet. Skal man være sikret samme adresse, må dette avtales med nettleverandøren. I de tilfeller der det ikke

[6] Lov 4. august 1995 nr. 53, politil

foreligger slik avtale, er det vanskelig å identifisere en bestemt maskin. Samtidig har trådløse nettverkskort blitt populære. Disse kortene gjør at man slipper alle ledningene og koblingene, noe som gjør at datamaskinen blir mer mobil. Ved hjelp av et slikt kort kan man koble seg opp hvor som helst innenfor en bestemt radius av nettverksruteren. Imidlertid er disse kortene lette å "hacke" seg inn på. Eksempelvis kan man få inn naboens nett dersom han har trådløst nettverk. I og med at det er hans nettilgang, er det hans IP-adresse som kan avleses i internettprotokollene. For å unngå slik inntrengning, må man installere et krypteringsprogram og en brannmur.

Ved hjelp av enkle grep er det nå mulig å ringe gjennom nettet, enten til en datamaskin eller til en telefon. Eksperter spår at IP-telefoni er det nye store innenfor kommunikasjonsanlegg. For å benytte seg av denne tjenesten, må en ha bredbåndsnett. Telefonen kobles så opp mot nettet slik at en ringer på bredbåndslinja. En kan også ringe gjennom en datamaskin. Det finnes ulike programmer en kan laste ned gratis fra nettet. Ved hjelp av dette programmet kan en ringe fra egen maskin til en annen maskin, eventuelt en telefon. I begge tilfellene identifiseres man ved IP-adressen.

Mobiltelefon (GSM), identifiseres i praksis ved hjelp av telefonnummer. I tillegg er telefonene fra fabrikken utstyrt med et individuelt serienummer, et såkalt IMEI-nummer (International Mobile Equipment Identity). Dette nummeret viser til én bestemt telefon. For å kunne bruke en mobiltelefon må man ha et SIM-kort. Det er dette kortet som formidler all kontakt med nettleverandør og dermed all kommunikasjon ut. SIM-kortet er også utstyrt med et nummer, IMSI (International Mobile Subscriber Identity). Dette nummeret angir abonnenten som er registrert på telefonens SIM-kort.

1.4 Rettstilstanden før ikrafttredelsen av de nye reglene

I Norge har man lenge godtatt bruk av kommunikasjonskontroll. Allerede i september 1939 førte Handelsdepartementet kontroll med telegraf, telefon og radiokorrespondansen i medhold av fullmakt.[7] Departementet kunne også fastsette innskrenkninger i

[7] Bergh og Eriksen, "Overvåking i Norge 1914-1997 Bind I" side 55

korrespondansen i den utstrekning det måtte være påkrevd for rikets sikkerhet. Dette som følge av stemningen i tiden før utbruddet av andre verdenskrig. Som en midlertidig ordning åpnet lov av 17. desember 1976 nr. 99 for telefonavlytting i narkotikasaker. Lovens gyldighetstid ble forlenget flere ganger. Ved lov av 5. juni 1992 nr. 52 ble hjemlene overført til straffeprosessloven og gjort permanente.[8] Hjemmelen har senere blitt utvidet til også å omfatte andre saker av særlig alvorlighet. Kriminalitetskravet vil bli behandlet nærmere i 2.1.7.

Samtidig som politiet har hatt omfattende hjemmel til å begjære kontroll med kommunikasjonsanlegg, har teknologien på enkelte områder utviklet seg på tvers av lovens vilkår. Særlig gjelder dette mobiltelefoner, og til dels datamaskiner koblet til nett. Som nevnt ovenfor stiller loven krav om at det anlegg som skal avlyttes må identifiseres entydig. Politiet kan med andre ord ikke begjære avlytting av telefoner som det må antas at mistenkte generelt har befatning med.

De siste årene har kontantkort til mobiltelefoner vokst frem som et populært alternativ til abonnement typene med fast månedspris. Kontantkort er et forhåndsbetalt kort, som gjør at man kan utføre teletjenester innenfor et begrenset beløp. Det begrensede beløpet tilsvarer det som til enhver tid er forhåndsbetalt. Inntil for kort tid siden var det mulig å erverve et slikt kort anonymt, noe som førte til at mange kriminelle var i besittelse av opptil flere slike telefoner.[9] SIM-kortet var ikke nødvendigvis registrert på reelle personer, noe som gjorde det vanskelig for politiet å finne frem til de telefoner man ønsket å avlytte. Politiet måtte ta i bruk registersøk og analyse, samt tradisjonell observasjon og spaning for å finne frem til anleggets identitet. Dette var tidkrevende arbeid, og ofte ble politiet ”hengende etter”. Når

[8] Ot.prp. nr. 13 (1990-1991) om lov om endringer i midlertidig lov 17. desember 1976 nr. 99 om adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivningen, samt Ot.prp. nr. 40 (1991-1992) om lov om endringer i straffeprosessloven (telefonavlytting i narkotikasaker).

[9] Post- og teletilsynet vedtok i november 2004 et forbud mot uregistrerte kontantkorttelefoner blant annet på bakgrunn av at det var vanskelig å få iverksatt telefonavlytting. Før 1. februar i år måtte alle telefonene være registrert.

de endelig hadde funnet frem til rett identitet, hadde de mistenkte allerede ny telefon. Dette førte til forsinkelser i etterforskningen, i forbindelse med pågripelse og eventuelle andre tiltak.

Det er grunn til å tro at selv om det ikke lenger er mulig å registrere kontantkort anonymt, klarer kriminelle miljø å omgå registreringsplikten. Dette kommer i tillegg til at noen kontantkort kun brukes en gang, samt at det benyttes stjålne og lånte telefoner. Behovet for reglene om identifikasjon av kommunikasjonsanlegg er derfor til stede, også etter at det ikke lengre er mulig å registrere kontantkort uten personalia

Før 5. august 2005 var det ikke hjemmel i lov til å iverksette identifikasjon av ukjente kommunikasjonsanlegg. Dette har ikke bare skapt forsinkelser og vanskeligheter i forbindelse med etterforskningen av straffbare handlinger, i tillegg har det gått med store ressurser for å finne frem til identiteten på det aktuelle anlegget. Det er håp om at de nye reglene kan frigjøre ressurser, som igjen kan settes inn på andre områder med stort behov. Reglene forutsettes derfor å kunne gi en effektivitetsgevinst.

1.5 Legalitetsprinsippet som skranke

Det er ikke tvil om at kommunikasjonskontroll generelt krever hjemmel i lov. Slike tiltak er så inngripende ovenfor den enkelte, at myndighetsutøvelse av denne typen må bygge på fullmakt gitt av Stortinget i lovs form. Det samme må gjelde for de nye reglene. Dette følger både av det internrettslige legalitetsprinsipp og av kravet til lovhjemmel i EMK art. 8. Lovkravet etter EMK art. 8 vil bli behandlet nærmere i 3.2.1.

Det internrettslige legalitetsprinsipp er i stor grad bygget på ulovfestet rett av grunnlovs rang, altså konstitusjonell sedvane.[10] Enkeltstående utslag av legalitetsprinsippet finner man i Grunnloven §§ 96, 99.[11] Noe upresist kan en si at inngrep i borgernes rettssfære (eks.

[10] Nærmere behandling av legalitetsprinsippet, se Eckhoff 2003

[11] Lov 17. mai 1814 (Grl.)

eiendomsrett og alminnelig handlefrihet) trenger hjemmel i lov. Mer presist følger legalitetsprinsippet av rettsstatsprinsippet alle moderne konstitusjoner bygger på; skal en beslutning ha rettslig bindende kraft slik at den kan legges til grunn for domstoler og andre offentlige myndigheter, må den bygge på en rettsregel med bindende virkning.[12] Prinsippet er også utslag av maktfordelingsprinsippet og folkesuverenitetsprinsippet.

Kravet til lovhjemmel varierer etter hvilket område en befinner seg på. Eksempelvis skal det på områder som angår den personlige frihet, lite til før det kreves uttrykkelig lovhjemmel. Situasjonen har vært en annen når det gjelder retten til privatliv. På mange måter har den psykiske integriteten, i motsetning til den fysiske, lidt under at politiet har hatt ganske frie tøyler etter den alminnelige handlefrihet. Selv om identifisering av kommunikasjonsanlegg rammer den psykiske integritet, kan det ikke være tvil om at identifiseringen faller inn under de tvangsmidler som krever uttrykkelig lovhjemmel, også i medhold av legalitetsprinsippet. Det internrettslige legalitetsprinsipp vil ikke bli behandlet nærmere, da EMK art. 8 oppstiller eget lovkrav.

1.6 Straffeprosessuelle utgangspunkter

Til grunn for straffeprosessen ligger det en lang rekke grunnprinsipper. På sett og vis kan man se på grunnprinsippene som rettssikkerhetsgarantier. Disse prinsippene skal ivareta bestemte hensyn som kontradiksjon, offentlighet og partsoffentlighet.[13]

Kontradiksjonsprinsippet er først og fremst en rett til å uttale seg. Dette skal bidra til sakens opplysning og øke sannsynligheten for en mest mulig materielt riktig avgjørelse. Prinsippet har gitt utslag i en rekke lovbestemmelser, blant annet strpl. § 92 første ledd annet punktum. I forbindelse med bruk av hemmelige tvangsmidler er det viktig at mistenkte ikke får varsel om iverksettelsen av tiltakene. Etter strpl. § 216 e annet ledd skal verken mistenkte eller andre avgjørelsen retter seg mot, eksempelvis tredjemann som er innehaver

[12] Se nærmere om dette i Bernt og Rasmussen 2003 B. 1 kapittel 1.

[13] Behandlet i Hov 1999, Rettergang I kapittel 3

av telefonabonnementet, få melding om avgjørelse eller få rett til å uttale seg. Blir en person varslet om avlytting, vil han kunne ta sine forholdsregler. Konsekvent gjennomføring av kontradiksjon er derfor ikke mulig.

Etter strpl. § 100 a skal det oppnevnes en forsvarer som skal ivareta mistenktes interesser under rettens behandling av begjæringen. Det er forutsatt i forarbeidene at forsvareren skal være aktiv og spørrende ovenfor påtalemyndigheten.[14] Ordningen skal sikre at avlyttingen er undergitt reell kontroll. Forsvareren skal kunne se og uttale seg om materialet som foreligger. Det vil ellers være vanskelig å vurdere hvorvidt mistankekravet er oppfylt. Det er imidlertid kun dommeren som av særlige grunner kan be om å få forelagt alle dokumenter. Forsvareren har kun krav på de rapporter politiet legger frem som begrunnelse.[15] Heller ikke kan forsvareren innhente informasjon fra mistenkte eller vitner i og med at kontrollen skal være hemmelig. Når dette er tilfellet kan man stille spørsmålstegn ved om kontradiksjonen virkelig blir ivaretatt. Forsvarerne skal forsvare mistenkte og ivareta hans interesser, men det blir en nesten umulig oppgave under de rådende forhold. Advokat Knut Rognlien skriver i en artikkel at flere forsvarere føler seg som gisler i avlyttingssakene. Politiet opplyser bare at de ”vet” noe, og at domstolene gir tillatelse til kommunikasjonskontroll i tillit til at politiet ikke iverksetter slik kontroll uten å ha god grunn til det.[16] Heller ikke i de tilfeller der det blir gitt avslag på begjæring om tvangsmidler blir mistenkte og hans advokat varslet. I og med at dette kan forspille formålet med selve kontrolltiltaket, og følger av strpl. § 381 tredje ledd annet punktum.

I saker om kommunikasjonskontroll er utgangspunktet at den mistenkte ikke har anledning til å gjøre seg kjent med de opplysninger som domstolen legger til grunn. Utenfor disse

---

[14] Ot.prp. nr. 64 (1998-99) Om lov om endringer i straffeprosessloven og straffeloven m.v. (etterforskningsmetoder m.v.), side 144

[15] Sanksjonert tolkning i en enstemmig avgjørelse fra Høyesteretts kjæremålsutvalg fra 2003, avgjørelsen er omtalt i John Christian Eldens ytring (”Om personvern, avlytting og politistat”) i Tidsskrift for strafferett (2005).

[16]”Advokater som gisler i telefonavlyttingssaker” (Rognlien 2004)

sakene er utgangspunktet det motsatte, dette for å sikre kontradiksjon (prinsippet om partsoffentlighet). Verken den mistenkte eller hans advokat skal vite om kontrolltiltaket, dokumentinnsyn er derfor utelukket. Dette må sees i sammenheng med "den hemmelige forsvareren" som blir oppnevnt etter strpl. § 100 a. En annen ting er at den som blir utsatt for hemmelig avlytting etter strpl. kapittel. 16 a, heller ikke får stilling som siktet jf. strpl. § 82 tredje ledd første punktum jf. § 216 e annet ledd.[17] En mistenkt har, etter straffeprosesslovens regler, ikke innsynsrett i saksdokumenter. Det bemerkes til slutt at det etter forvaltningsloven § 4 b) gjøres unntak for saker politiet behandler eller avgjør etter rettspleielovgivningen, herunder straffeprosessloven.[18]

Det er også prinsipielt viktig at det er åpenhet rundt rettssaker, også kalt prinsippet om offentlighet. Publikum skal ha en generell mulighet til å gjøre seg kjent med det som skjer. Dette skal styrke tilliten til rettsvesenet ved at publikum og presse kan følge rettsmøtene. Etter offentlighetsloven § 6 nr. 5 gjelder det intet generelt offentlighetsprinsipp for påtalemyndighetens virksomhet jf. unntak for *"[a]nmeldelse, rapport og annet dokument om lovovertredelse"*.[19] Dette følger også av strpl. § 61 a jf. påtaleinstruksen kapittel. 3 om alminnelig taushetsplikt for tjenestemann i politiet eller påtalemyndigheten.[20] For kontroll av kommunikasjonsanlegg etter strpl. kapittel. 16 a, følger dette av strpl. § 216 i. Etter bestemmelsen skal alle bevare taushet om begjæring av kommunikasjonskontroll og opplysninger som fremkommer under eller i forbindelse med kontrollen. Offentlighet vil kunne ødelegge etterforskningen og være belastende for de personer etterforskningen angår.

---

[17] For nærmere om dette se Ot.prp. nr. 40 (1991-92) punkt 3.3.3

[18] Lov om behandlingsmåten i forvaltningssaker, 10. februar 1967

[19] Lov om offentlighet i forvaltningen, 19.juni nr. 69 1970

[20] Forskrift om ordningen av påtalemyndigheten (påtaleinstruksen), fastsatt ved kongelig resolusjon 28. juni 1985 nr. 1679 i medhold av strpl. § 62

1.7 Forebyggende og avvergende politivirksomhet

Etter strpl. §§ 216 a og 216 b har ikke politiet adgang til å benytte seg av kommunikasjonskontroll ved avverging eller forebygging av kriminelle handlinger. Adgangen til å iverksette tiltak etter strpl. kapittel 16 a, kan kun brukes der man har mistanke om handling eller forsøk på handling. Bestemmelsen forutsetter dermed at den kriminelle handling er påbegynt eller allerede fullført, eventuelt forsøkt påbegynt eller fullført. Det er ikke tvil om at politiet også på andre stadier, for eksempel på avvergings- eller forebyggingsstadiet, har behov for å benytte seg av slike tiltak som beskrevet i strpl. §§ 216 a og 216 b. Med avverging av handling forstås tiltak som iverksettes forut for gjerningstidspunktet, men likevel umiddelbart før handlingen ellers ville blitt begått. Med forebygging av handling forstås tiltak som settes i gang mens handlingen ennå befinner seg på forberedelsesstadiet.

Ved lovendringen i august 2005, ble det inntatt en avvergingshjemmel i § 222 d i nytt kapittel 17 b ” Bruk av tvangsmidler for å avverge alvorlig kriminalitet” i strpl. Bestemmelsen gir politiet adgang til å iverksette tiltak som nevnt i strpl. kapittel 16 a, dersom politiet har rimelig grunn til å tro at noen kommer til å begå en kriminell handling av en viss alvorlighet. For mer om kriminalitetskravet, se 2.1.7. I forbindelse med lovendringen, ble også politiloven endret. Det ble inntatt et nytt kapittel III A ” Adgangen for Politiets sikkerhetstjeneste til å bruke tvangsmidler i forebyggende øyemed”. Politiets sikkerhetstjeneste (PST) er etter dette på nærmere bestemte vilkår gitt anledning til å iverksette kommunikasjonskontroll blant annet som nevnt i strpl. §§ 216 a og 216 b. Dersom det er grunn til å undersøke om noen forbereder en kriminell handling av en viss alvorlighetsgrad, kan PST sette i gang identifikasjon og avlytting av kommunikasjonsanlegg. Tidsmessig vil etterforskning og tvangsmiddelbruk etter disse hjemlene være forut for etterforskning og tvangsmiddelbruk etter strpl. kapittel 16 a. I det følgende vil behandlingen av den materielle rett konsentrere seg om adgangen til å iverksette kommunikasjonskontroll etter strpl. kapittel 16 a i forbindelse med allerede fullførte handlinger.

1.8 Forholdet til lov om elektronisk kommunikasjon (ekoml.) § 2-9 tredje ledd jf. fjerde ledd

Ekomloven har i følge lovens § 1-1, som formål *"…å sikre brukerne i hele landet gode, rimelige og fremtidsrettede elektroniske kommunikasjonstjenester, gjennom effektiv bruk av samfunnets ressurser…"*.[21] Lovens § 2-9 bestemmer at tilbyder og installatør og andre som arbeider eller utfører tjenester for dem, har taushetsplikt hva angår innholdet i, og andres bruk av, elektronisk kommunikasjon. De plikter også å gjennomføre tiltak for å hindre at andre enn de opplysningene gjelder, kan få kjennskap til dem. Dette skulle bety at nettilbyder kan motsette seg å gi opplysninger som politiet måtte ønske i forbindelse med en etterforskning. Ekomloven § 2-9 tredje ledd åpner imidlertid for at det til påtalemyndigheten eller politiet kan gis opplysninger om avtalebaserte hemmelige telefonnumre, elektronisk kommunikasjonsadresse og andre abonnementsopplysninger. "Andre abonnementsopplysninger" vil for eksempel være navn, adresse, SIM-kortnummer, IMEI-nummer eller IMSI-nummer, men også fra hvilket telefonnummer et internettabonnement er opprettet fra. Med den nye hjemmelen vil politiet kunne innhente numrene uten tilbyders medvirkning. For så i neste omgang, dersom opplysningene gir tilstrekkelig grunnlag, å bruke dem til beslutning om innsyn i abonnementsopplysninger og utleveringspålegg for å innhente historiske og fremtidige trafikk- og lokaliseringsdata.

Opplysninger etter ekomloven § 2-9 tredje ledd kan likevel ikke gis ut ubegrenset. Fjerde ledd bestemmer at dersom særlige forhold gjør det utilrådelig, skal ikke påtalemyndigheten eller politiet få tilgang til opplysningene. Det er ikke klart hva som regnes som "utilrådelig", men det vil for eksempel kunne være aktuelt i forbindelse med opplysninger som politiet anmoder om utenfor etterforskning. Dette vil være saker i forbindelse med politiets sivile oppgaver, som forvaltningsoppgaver og arbeidet med namssaker.[22] Spørsmålet blir så hva som regnes som særlige forhold. Ordlyden tilsier at det

[21] Lov 4. juli 2003 nr. 83, ekomloven

[22] Se nærmere om dette i Ot.prp. nr. 58 (2002-2003) punkt 16 om generelle bemerkninger til ekoml. § 2-9, som viser til Ot.prp. nr. 31 (1997-1998) endringer i lov om telekommunikasjon, punkt 3.6 side 8.

må være en snever unntaksregel, slik at det kun i svært få tilfeller vil være tilrådelig å holde opplysninger tilbake. Eksempelvis der politiets informasjon ikke er tilstrekkelig til entydig å utpeke en abonnent. Entydig vil her si for eksempel dynamisk IP-adresse med eksakt påloggingstidspunkt.

1.9 Metode

1.9.1 Lex superior- og forrangsprinsippet

Norsk rett har ulike trinnhøyder for rettsregler, lex superior-prinsippet. Prinsippet er et verktøy for lettere å kunne løse motstrid mellom reglene. En regels trinnhøyde bestemmer hvilken regel som skal gå foran i tilfelle motstrid. Avveiningen er ikke skjønnsmessig, den regel som har høyest rang går foran. Dette gjelder uansett om den er mer eller mindre spesiell eller om den er gitt først eller sist. Rangen bestemmes av hvilken kompetanseregel den er gitt i medhold av, slik at alle regler gitt i medhold av en bestemt kompetanseregel vil ha samme rang. Kompetanseregelen selv vil ha høyere rang enn de regler som blir gitt i medhold av den. Med unntak av Grunnloven, har alle formelle lover samme rang. Grunnloven er lex superior, da all formell lov har hjemmel her.[23]

Ved Grunnlovsbestemmelse av 15. juli 1994 nr. 675 ble det tilføyd en ny Grl. § 110 c.[24]
"Det paaligger Statens Myndigheder at respektere og sikre Menneskerettighederne. Nærmere Bestemmelser om Gjennemførelsen af Traktater herom fastsættes ved Lov."
Bestemmelsen har ikke bare symbolfunksjon, men har også et materielt innhold. Første ledd viser helt generelt til alle menneskerettighetskonvensjoner, men gir likevel myndighetene en rettslig bindende retningslinje. I tillegg vil første ledd legge bånd på forvaltningsorganer når de utøver myndighet etter fritt skjønn, og være et viktig tolkningsmoment for lovgivningen. Annet ledd er en videreføring av prinsippbestemmelsen

---

Ekoml. § 2-9 er en videreføring av den gamle bestemmelsen i telekommunikasjonsloven. Se også Rt. 1999 side 1944 særlig side 1949.

[23] Prinsippet er nærmere behandlet i Eckhoff 2001

[24] Behandlet i Møse 2002 side 178

i første ledd, og gir henvisning til lovgiver om å følge utviklingen og utarbeide lovregler som ledd i plikten til å sikre og respektere menneskerettighetene der det anses nødvendig. Annet ledd bestemmer at nærmere gjennomføringsregler for den enkelte konvensjon skal gjøres i lovform.[25] Menneskerettighetsloven § 2 inkorporerer EMK i norsk lov. Etter dette er EMK formell lov med rang under Grunnloven.

Det er likevel ikke klart om inkorporerte konvensjonsbestemmelser går foran Grl. der det skulle oppstå motstrid. Det finnes lite skrevet på området, og det er lite praksis som gir veiledning. I forarbeidene finnes det støtte for å tolke "annen lovgiving" slik at Grl. unntas. Forarbeidene diskuterer hvorvidt konvensjonene skal gis grunnlovs kraft, og eventuelle konsekvenser av dette. Det pekes blant annet på at norske lovgivingsmyndigheter vil respektere folkerettslige forpliktelser uansett om de er innarbeidet i lovs eller grunnlovs form, og neppe vedta regler i strid med disse.[26] Når nå konvensjonen er inntatt i formell lov ved hjelp av inkorporasjon, peker dette i retning av at Grl. går foran menneskerettighetskonvensjonene ved eventuell motstrid. Etter dette befinner konvensjonen seg i en slags mellomstilling mellom formell lov og Grunnloven, semikonstitusjonell.

Etter mnskrl. § 3 skal bestemmelser i EMK og tilleggsprotokollene ved motstrid gå foran annen lovgivning.[27] Dette følger også av strpl. § 4 "*lovens regler gjelder med de begrensninger som er anerkjent i folkeretten eller følger av overenskomst med fremmed stat*". Det har imidlertid vært noe usikkert hvorvidt de folkerettslige reglene skulle gå foran ved enhver motstrid. Temaet har vært oppe i flere Høyesterettsdommer, og fikk først sin avklaring ved plenumsdommen inntatt i Rt. 2000 side 996 (Bøhler-saken).

---

[25] For nærmere redegjørelse for Grl. § 100 c, se NOU 1993:18 Lovgivning om menneskerettigheter, punkt 11.3.3 side 157-160.

[26] Se nærmere NOU 1993:18 punkt 10.4 "Inkorporerte menneskerettighetskonvensjoners trinnhøyde"

[27] Temaet er behandlet i Møse 2002 side 176 flg.

Bøhler-saken gjaldt spørsmål om adgang til å ilegge tilleggsskatt, og hvorvidt tilleggsskatt var å anse som straff i forhold til EMK art. 6. Dersom tilleggsskatten var å anse som straff, ville EMK ha forrang i forhold til de norske reglene? Høyesterett uttaler på side 1006 følgende at det i mange tilfeller kan være tvil om hvordan EMK skal forstås. Tilsynelatende motstrid vil ikke kunne løses ved hjelp av et generelt prinsipp, men vil måtte bero på en nærmere tolkning av de aktuelle rettsregler. Norske domstoler må forholde seg til EMK og benytte de samme tolkningsprinsipp som Den europeiske menneskerettighetsdomstol (EMD), men det er EMD som skal utvikle konvensjonen. Ved at det ved avveiningen av ulike interesser og verdier kan bygges på norske verdioppfatninger, vil de kunne inngå i samspill med EMD og påvirke dens praksis. ”Dersom norske domstoler skulle være like dynamiske i sin fortolkning av EMK som det EMD er, ville man risikere at norske domstoler i enkelte tilfelle går lenger enn det som er nødvendig i forhold til EMK. … Som alminnelig regel kan norske domstoler ved tolkningen av EMK heller ikke bygge inn sikkerhetsmarginer mot at Norge dømmes for konvensjonsbrudd.” Dersom tolkningen av en konvensjonsbestemmelse har de beste grunner for seg, men strider med norsk intern rett, vil konvensjonsbestemmelsen gå foran den norske regelen jamfør ordlyden i mnskrl. § 3. Dette ble også slått fast i Dobbeltstraff I-saken på side 565, der førstvoterende henviser til Bøhler-saken og uttaler at det ikke kreves at konvensjonstolkningen fremstår som ”rimelig klar” for at konvensjonsbestemmelsen skal gå foran norsk intern rett.[28]

1.9.2 Tolking av EMK

Ovenfor er det sagt at norske domstoler må legge til grunn de samme tolkingsprinsipper som EMD ved tolkningen av EMK. Dette er også tema i et rundskriv fra Justisdepartementet, G-45/99. Nedenfor følger en innføring i tolkning av EMK. Et generelt utgangspunkt for tolking av EMK er Wien-konvensjonen art. 31.[29] Wien-konvensjonen eksisterte ikke da EMK ble vedtatt, og etter Wien-konvensjonen art. 4 har ikke

[28] Rt. 2002 side 509, også denne saken gjaldt overprøving av ileggelse av tilleggsskatt etter ligningsloven § 10-2 jf 10-4 nr. 1, 1. punktum var straff etter EMK art. 6 (1)

[29] Wien-konvensjonen (Vienna Convention on the Law of Treaties) av 23. mai 1969

konvensjonen tilbakevirkende kraft. Konvensjonen er heller ikke ratifisert av Norge. Dette har imidlertid ingen reell betydning, da konvensjonen i all vesentlig grad kodifiserer ulovfestet tolkningslære i folkeretten.

Etter Wien-konvensjonen art. 31 første ledd er ordlydens naturlige eller vanlige mening utgangspunkt ved traktattolkning. I forbindelse med vanlig språklig betydning, må en imidlertid huske at EMK inneholder autonome begreper for å sikre individenes vern. Dersom man ikke la til grunn en autonom tolkning av begrepene, ville individene i verste fall ha ulikt vern i de forskjellige landene fordi de enkelte stater ikke nødvendigvis har sammenfallende definisjoner. Dette ville stride med prinsippet om at rettighetene er universelle. Naturlig utgangspunkt for tolkningen vil da være betydningen av ordene da traktaten ble til. På menneskerettighetsområdet blir dette likevel unøyaktig, da samfunnsforholdene til stadighet endrer seg og hvor man kanskje nettopp derfor har et større behov for dynamisk tolkning av begrepene. EMD har da også i flere tilfeller lagt til grunn at konvensjonen må tolkes på bakgrunn av de herskende samfunnsforhold, se eksempelvis Dudgeon v. the United Kingdom avsnitt 60.[30]

Avgjørelser fra EMD vil ha generell betydning ut over den konkrete sak, selv om Wien-konvensjonen kun anerkjenner tidligere praksis som subsidiære kilder. Av hensyn til forutberegnelighet og konsekvens bør derimot rettspraksis tillegges betydelig vekt. EMD fastlegger innholdet i vage ord, og legger til grunn retningslinjer som så gjentas og videreutvikles i sak etter sak. Presedensene er derfor autoritative rettskildefaktorer. Fordi konvensjonen er vagt utformet er det viktig at norske domstoler legger til grunn disse retningslinjene, og gir prejudikatene betydelig vekt i tolkningen av EMK. På denne måten er konvensjonene rettssettende og begrenser statenes suverenitet. Dette er også forutsatt i NOU 1993:18 punkt 13.2.2 om konvensjonsorganenes praksis.

---

[30] A 45 (1981) avsnitt 54, saken gjaldt hvorvidt reglene som gjorde homoseksuelle handlinger straffbare i Nord-Irland var i strid med art. 8. Se også 3.2.3 om vurderingen av nødvendigheten av reglene i et demokratisk samfunn.

EMDs praksis viser også at formålsbetraktninger blir tillagt betydelig vekt. Det kan dreie seg om formål som ligger til grunn for hele konvensjonen eventuelt kun en enkelt bestemmelse. Eksempel på slikt formål er å sikre og beskytte individenes menneskerettigheter. Etter konvensjonen er det er formål i seg selv å videreutvikle og fremme verdiene som ligger til grunn for dette. Dette må også sees i lys av at konvensjonen skal tolkes som et levende og dynamisk instrument som endrer seg med tiden og samfunnsforholdene ellers. Men der samfunnsforholdene ikke har endret seg er det heller ikke grunn til å endre en etablert tolkning av konvensjonen. Selv om formålet er å beskytte individene, har EMD i flere tilfeller latt hensynet til statens interesser påvirke tolkningen. Eksempelvis sterke reelle hensyn som taler for en bestemt tolkning.

Etter Wien-konvensjonen er forarbeidene bare supplerende rettskilder jamfør art. 32. EMD praksis viser imidlertid at forarbeidene brukes som tolkningsmidler. Rett nok er forarbeidene mer enn 40 år gamle, og de vil til en viss grad være fortrengt, i og med at EMK tolkes dynamisk i lys av de rådende samfunnsforhold. En vil derfor kunne si at forarbeidene likevel kun er av avgjørende betydning der rettsanvenderen ikke har avgjørende holdepunkter i andre rettskilder.[31]

[31] For mer detaljert behandling av tolkingen av EMK, se for eksempel Aall 1995 og Frode Elgesem i Lov og Rett 2003 side 203.

2 Presentasjon av vilkårene for identifisering

Straffeloven § 145 a bestemmer at det er straffbart å hemmelig avlytte eller ta opp telefonsamtaler som man selv ikke deltar i. Bestemmelsen gjelder også for politiet under etterforskningen hvis ikke politiet har særskilt hjemmel til å foreta kommunikasjonskontroll. Slik hjemmel finnes i straffeprosessloven kapittel 16 a. Etter alminnelig språkforståelse vil ikke identifisering av et kommunikasjonsanlegg umiddelbart være det samme som kontroll av det. Imidlertid blir de to begrepene likestilt i strpl. §§ 216 a tredje ledd annet punktum og 216 b annet ledd litra c). Under følger derfor en fremstilling av de ulike vilkårene i bestemmelsene.

2.1 Materielle vilkår for iverksetting av identifisering etter strpl. §§ 216 a og 216 b

2.1.1 Fullbyrdet handling eller forsøk på handling

Straffeprosessloven § 216 a første ledd første setning lyder som følger; *"[r]etten kan ved kjennelse gi politiet tillatelse til å foreta kommunikasjonsavlytting når noen med skjellig grunn mistenkes for en handling eller forsøk på handling…"*. Det samme følger av strpl. § 216 b første ledd første setning. Både strpl. §§ 216 a og 216 b likestiller fullbyrdet handling og forsøk på handling. En handling er fullbyrdet når den kan sies å dekke de objektive elementene i gjerningsbeskrivelsen i et straffebud. Straffbart forsøk er definert i strl. § 49. Etter dette er et forsøk straffbart når en handling ikke er fullbyrdet, men det er foretatt noe som kan tyde på at den straffbare handling kan sies å være påbegynt. På denne måten kan det iverksettes metoder før hele handlingen dekker hele gjerningsbeskrivelsen. Det må imidlertid trekkes en grense mot den nedre grense for straffri forberedelse. Adgang til identifisering er ikke mulig så lenge den mistenkte fortsatt er på det rene forberedelsesstadiet.

Den nedre grense for straffbart forsøk er ikke fastlagt i lov, men har fått et nærmere innhold gjennom rettspraksis. Blant annet i "Parykkpyroman-dommen".[32] Saken gjaldt en tiltalt, som etter å ha parkert sin bil utenfor et lokale der det skulle åpnes en forretning i samme bransje som tiltalte selv drev i, spaserte rundt med parykk på hodet og en fyrstikkeske i lommen. Bakdøren i tiltaltes bil var åpen og det ble funnet en kanne bensin i bilen. Mannen ble frikjent for forsøk på skadeverk etter strl. § 291. Høyesterett uttaler på side 18 at "[e]t moment i grensedragningen mellom forsøk og straffri forberedelse er den psykologiske forskjell mellom det gjerningspersonen alt har gjort, og det som gjenstår å gjøre for at forbrytelsen skal være fullbyrdet. I saken her hadde gjerningsmannen utført flere forberedende handlinger,… Men viktige handlinger - fysisk og psykisk – stod også igjen… Etter min mening er det en nokså klar psykologisk forskjell mellom det han hadde gjort, og det som stod igjen." Etter dette er det klart at momenter i vurderingen hvorvidt den nedre grense er overtrådt, vil være et spørsmål om hvor langt vedkommende er kommet i tid, rom og mentalt, altså hvor stor den psykologiske terskelen til fullført handling er.[33]

Det fremgår ikke av lovteksten hvorvidt det kan begjæres identifikasjon av medvirker til slik handling som nevnt i strpl. §§ 216 a og 216 b bestemmelsenes første ledd og som kan gi grunnlag for kontroll. Det finnes ingen generell regel i straffeloven som kriminaliserer en medvirkningshandling. Hvorvidt medvirkningshandlingen er straffbar i de tilfeller der medvirkningen ikke eksplisitt er gjort straffbar, må avgjøres etter en tolkning av det enkelte straffebud. En rimelig tolkning av strpl. §§ 216 a og 216 b er at også medvirker kan risikere identifisering og kontroll av sine anlegg. En medvirker kan også mistenkes for en straffbar handling eller forsøk på slik handling. Derimot er det ikke adgang til å bruke etterforskningsmetoder mot hovedmannen dersom ikke også denne har overskredet den nedre grensen for straffbart forsøk.

---

[32] Rt. 1995 side 17

[33] For nærmere redegjørelse av den nedre grense, se eksempelvis Eskeland 2000 side 204 flg. Se også Bjerke 1990, særlig side 214-215.

2.1.2 Hvilke kommunikasjonsanlegg kan identifiseres?

Det fremkommer av strpl. §§ 216 a tredje ledd og 216 b annet ledd at det som kan begjæres identifisert er telefoner, datamaskiner eller andre anlegg for elektronisk kommunikasjon. Det mest praktiske er datamaskiner og telefoner, herunder både fasttelefon og mobiltelefon. Begrepet "andre anlegg for elektronisk kommunikasjon" er heller ikke helt upraktisk, men begrepet er meget vidt. "Andre anlegg" vil typisk være telefaks, personsøker (mini-link), teleks og videooverføringer med lyd.[34] I teorien kan en også tenke seg identifisering av walkietalkie, men dette er upraktisk da få benytter seg av dette kommunikasjonsanlegget i dagliglivet. Med et så vidt begrep kan eventuelle fremtidige nyvinninger på kommunikasjonsområdet også omfattes, slik at man i fremtiden slipper lovendring.

Interne anlegg, som callinganlegg i oppganger eller hustelefoner omfattes ikke av begrepet. I NOU 1997:15 blir det lagt til grunn at disse anleggene har en annen funksjon enn andre kommunikasjonsanlegg. Hensynet bak et callinganlegg er "å spare brukerne for å måtte gå inn i et annet lokale for å snakke med vedkommende".[35] Identifisering av slike anlegg må skje etter reglene for romavlytting etter strpl. § 216 m. Bestemmelsen innholder ingen regler for identifisering av anlegg. Strpl. § 216 a forutsetter at informasjon sendes til eksterne anlegg.

Etter bestemmelsens ordlyd er det bare kommunikasjonsanlegg "som den mistenkte besitter eller kan antas å ville bruke" som kan identifiseres. Kravet til besittelse betyr at mistenkte ikke behøver å være eier av anlegget. Med "*bruke*" menes direkte bruk. Anlegget kan være både lånt eller leid. Begrepet *"antas å ville bruke"* henspeiler til en objektiv vurdering med konkrete holdepunkter. Det bør være en viss sannsynlighet for at mistenkte vil benytte seg

---

[34] Per i dag finnes det ikke lengre nett for teleks i Norge. Imidlertid er det mange andre land der teleks fortsatt brukes mye. For bedrifter i Norge tilbyr derfor enkelte teleselskaper, blant annet Telenor, en tjeneste der e-poster blir transformert til teleks når de kommer frem til mottakeren. Fra og med 1.9.2003 finnes det heller ikke lengre nett for personsøker og mini-link. Bakgrunnen for dette er at mobiltelefonene har tatt over behovet for kommunikasjonsanlegg av denne typen.

[35] NOU 1997:15 Etterforskningsmetoder for bekjempelse av kriminalitet punkt 4.2.5.3 side 66

av anlegget. Det kreves likevel ikke sannsynlighetsovervekt. Videre forutsettes det at det kun er mistenktes anlegg som skal kunne identifiseres. Anlegg som mistenkte kommuniserer med, altså mottaker, kan ikke identifiseres.[36]

2.1.3 Begrepet "kommunikasjonsavlytting"

Etter strpl. § 216 a tredje ledd kan kommunikasjonsavlytting bestå i å avlytte samtaler eller annen form for kommunikasjon mellom kommunikasjonsanlegg. Både SMS og elektronisk post (e-post) kan avleses. Imidlertid er det begrensinger for hvilken kommunikasjonsstrøm som kan kontrolleres. Kun samtaler som føres mens avlytting pågår kan kontrolleres. Innleste beskjeder på telefonsvarer og mobilsvar faller derfor utenfor. Det samme må gjelde sendte SMS og lagrede e-poster.[37] Likeledes meldinger og e-poster som er sendt, men som ennå ikke har kommet frem til mottaker. Disse er lagret hos nettilbyder eksempelvis fordi telefonen er uten dekning eller det er forsinkelser på nettet, eller hele nettet er nede. Generelt må det gjelde at all lagret informasjon faller utenfor tillatelsen til kontroll.

I samsvar med det som er sagt ovenfor om interne anlegg som ikke lar seg identifisere og avlytte etter strpl. § 216 a, vil også kommunikasjon mellom egne anlegg falle utenfor, selv om de befinner seg på forskjellige steder. Med dette menes eksempelvis lagring av dokument på server, slik det gjøres på universitetet der studentene har eget hjemmeområde på en storserver og ikke på den bestemte maskinen de på det aktuelle tidspunkt jobber på.[38] Et annet eksempel vil være informasjon som er på vei fra datamaskin til printer.

Selve identifiseringen foregår ved fortløpende å lese av strømmen av signaler mellom kommunikasjonsanleggene mens formidlingen pågår. Signalstrømmen blir så omformet til meningsgivende data. Det stilles ikke krav til at den enkelte signalstrøm vil tilføre noe av

---

[36] Behandlet i Bjerke 2001 B. 1

[37] Se Bjerke 2001 B. 1 side 741

[38] Se NOU 1997:15 punkt 4.2.5

verdi for politiets arbeid, da avlytting blir iverksatt for en bestemt tidsperiode og ikke en enkelt signalstrøm-overføring.

Hvordan identifiseringen foregår, vil bli behandlet nedenfor i 2.2.1, selv om selve identifiseringen per definisjon også er kommunikasjonsavlytting.

2.1.4 Begrepet "annen kontroll"

Etter strpl. § 216 b første ledd vil *"annen kontroll"* være kontroll som ikke anses som kommunikasjonsavlytting etter strpl. § 216 a. I strpl. § 216 b er det listet opp en del tiltak som er å anse som annen kontroll etter første ledd. Listen i annet ledd kan ikke anses å være uttømmende, da det kun står *"kan"*. I teorien kan det derfor tenkes også andre tiltak som vil kunne falle inn under *"annen kontroll"*.

I henhold til annet ledd litra a) kan det dreie seg om å avbryte eller innstille kommunikasjon. Etter annet ledd litra b) kan en også stenge kommunikasjonsanlegg som beskrevet i kapittel 2.1.2. Annet ledd litra d) bestemmer at kontrollen også kan gå ut på å pålegge "eier eller tilbyder av nett eller tjeneste" å gi opplysninger om kommunikasjonsanlegg som har blitt satt, eller som skal bli satt, i forbindelse med anlegg som er under kontroll. Dette pålegget kan for øvrig bli iverksatt ovenfor enhver netteier eller tilbyder, enten det er snakk om privat eller offentlig nett- eller tjenesteleverandør.

Bestemmelsens annet ledd litra c) gir hjemmel til å identifisere kommunikasjonsanlegg som definert i 2.1.2. Identifisering etter bestemmelsen her vil bli behandlet i 2.2.2.

2.1.5 Beslutningskompetanse

Det er et krav etter både strpl. §§ 216 a og 216 b at begjæring om identifikasjon skal avgjøres av retten ved kjennelse. Tillatelsen må foreligge før en kan iverksette kommunikasjonskontroll. Dette er en viktig rettssikkerhetsgaranti, i det det er snakk om svært inngripende tiltak. Ved at tillatelse gis av retten, vil man kunne hindre at misbruk

skjer, og at hensyn både for og i mot kontroll blir tatt i betraktning. Retten er en nøytral instans som har generell tillitt i samfunnet.

I de tilfeller der det er stor fare for at etterforskingen kan ta skade av å vente på kjennelse fra retten, kan beslutning av påtalemyndigheten tre i stedet, såkalt hurtigkobling, jf. strpl. § 216 d. Beslutningen må imidlertid snartest mulig, og senest innen 24 timer fra da kontrollen ble iverksatt, legges frem for retten. Retten må altså uansett godkjenne kontrollen. Det kreves imidlertid ikke at retten har truffet avgjørelse innen 24-timers fristen, det er nok at begjæringen har blitt forelagt retten jf. Ot.prp. nr. 81 (1999-2000) side 46.[39] Dersom fristen går ut etter rettens ordinære kontortid, forlenges automatisk fristen til retten åpner igjen. Beslutning etter bestemmelsen her vil være mest aktuelt i helger og på helligdager.

Ordlyden reiser en rekke tolkningsspørsmål. Det er uklart hva "..er stor fare..", og "..etterforskningen vil lide.." innbærer. Det er nærliggende å tolke "lide" slik at etterforskningen kan bli vanskeliggjort og at viktig bevismateriale vil gå tapt dersom ikke identifisering iverksettes straks. Dette er forutsatt i Ot.prp. nr. 40 (1991-92) kapittel 7 side 41.[40] Identifisering etter bestemmelsen her kan ikke iverksettes av bekvemmelighetsgrunner. Når bestemmelsen bruker uttrykket "stor fare" må det sees i sammenheng med hvor sannsynlig det er at etterforskningen vil lide. Det må antakelig foreligge sannsynlighetsovervekt, både i forhold til den store faren selv og til viktigheten for etterforskningen.

Beslutningskompetanse i saker om hurtigkobling har politimesteren eller hans faste stedfortreder. Når avgjørelse blir tatt av stedfortreder, skal avgjørelsen så snart som mulig fremlegges for politimesteren for godkjenning jf. kommunikasjonskontrollforskriften § 2.[41] Denne kretsen kan også utvides, i det førstestatsadvokaten kan gi skriftlig samtykke til at

---

[39] Om lov om endringer i straffeloven og straffeprosessloven (bruken av varetektsfengsling mv.)

[40] Under bemerkninger til strpl. § 216 d.

[41] F31.03.1995 nr. 281 Forskrift om kommunikasjonskontroll (kommunikasjonskontrollforskriften)

andre (påtalemyndighetens) tjenestemenn i ledende stillinger kan inneha samme kompetanse som politimesterens stedfortreder. Hva menes så med "..påtalemyndighetens tjenestemenn i ledende stillinger.."? En rimelig tolkning er at det kun er tjenestemenn i ledende stillinger med juridisk embetseksamen som kan inneha kompetansen. Dette vil typisk være vakthavende politijurist eller påtaleleder, slik at for eksempel en politibetjent ikke kan ta avgjørelsen. Dette harmonerer også med språkbruken i strpl. § 55 der påtalemyndighetens tjenestemenn er oppramset, og i påtaleinstruksen § 22-2 der polititjenestemenn med juridisk embetseksamen kan ta ut tiltale.

2.1.6 Mistankekravet

Etter strpl. §§ 216a og 216b er det krav til skjellig grunn til mistanke for at tiltak skal kunne iverksettes.[42] Det kreves ikke sikker overbevisning om skyld (kvalifisert sannsynlighetsovervekt), men det er sikker rett at kravet innebærer sannsynlighetsovervekt. Dette er slått fast i praksis, blant annet i en kjennelse fra Høyesteretts kjæremålsutvalg inntatt i Rt. 1993 side 1302.[43] Av hensyn til forutberegnelighet og innrettelse, bør man legge til grunn at begrepet "*skjellig grunn*" forstås på samme måte overalt i straffeprosessloven. Ved vurdering av sannsynligheten må en blant annet se på om mistanken er forankret i objektive holdepunkter, for eksempel forklaringer eller andre bevis, og om bevisene til en viss grad av sannsynlighet peker ut den mistenkte. Det forutsettes at kravet til saklighet og rimelig grunn i forbindelse med åpningen av etterforsking er oppfylt jf. strpl. § 224.

[42] Behandlet i Hov 1999, Rettergang II side 49-50

[43] Saken gjaldt adgang til å pågripe og varetektsfengsle etter strpl. § 171

2.1.7 Kriminalitetskravet

Tidligere kunne man kun begjære kommunikasjonskontroll i forbindelse med narkotikaforbrytelser og i saker om rikets sikkerhet.[44] I 1999 ble ved lovendring bestemmelsens virkeområde utvidet.[45] Likevel kan det ikke iverksettes kommunikasjonskontroll i forbindelse med enhver forbrytelse. I det følgende vil de aktuelle straffebud bli kort presentert, utover dette vil ikke bestemmelsene bli behandlet.[46]

Etter strpl. §§ 216 a og 216 b stilles det krav til at den kriminelle handling er av en viss alvorlighet. Tillatelse kan imidlertid gis uavhengig av hva slags straffbar handling det er tale om, så fremt de andre materielle vilkår er oppfylt. Etter strpl. § 216 a første ledd litra a) kan det for handlinger som kan medføre fengsel i 10 år eller mer begjæres kontroll, for eksempel alvorlige allmennfarlige forbrytelser og grove seksualforbrytelser. Etter strpl. § 216 b første ledd litra a) er kravet 5 års fengsel eller mer, eksempelvis drap og grove legemsbeskadigelser. Det må være nok at strafferammen er nøyaktig 5 eller 10 år. Det er strafferammen i lovbestemmelsen en må se på, ikke hva mistenkte eventuelt ville fått i straff. Annet punktum i strpl. § 216 a bestemmer at det ikke skal tas i betraktning forhøyet straff i henhold til straffeloven § 61 som følge av gjentakelse av straffbart forhold.[47] Om dette sier forarbeidene at adgangen til kontroll ville blitt for stor dersom man skulle legge til grunn den utvidede straffen. "Utvalget finner… at hensynet til det integritetsinngrep telefonkontroll representerer og behovet for å opprettholde telefonkontroll som et ekstraordinært etterforskningsmiddel som unntaksvis benyttes der tradisjonell etterforsking forgjeves er forsøkt eller må anses som hensiktsløs, taler mot en slik utvidelse."[48] Derimot

---

[44] Før 1999 var kommunikasjonsavlytting i saker om rikets sikkerhet regulert i lov 24. juni 1915 nr. 5 om kontroll med post- og telegrafforsendelser og med telefon med tilhørende, samt tilhørende forskrift av 19. august 1960

[45] Endringslov 3. desember 1999 nr. 82

[46] Det finnes mye litteratur på området som gir en detaljert og utførlig behandling av bestemmelsene, se eksempelvis Johs. Andenæs, "Formuesforbrytelsene", Johs. Andenæs og Anders Bratholm "Spesiell strafferett" og Ståle Eskeland "Strafferett"

[47] Lov 22. mai 1902 nr. 10 (strl.)

[48] NOU 1997:15 avsnitt 6.2.1

bestemmer strl. § 60 a tredje ledd at forhøyning av maksimumstraff som følge av handling utøvd som ledd i virksomhet til organisert kriminell gruppe, skal tas i betraktning etter strpl. § 216 a. Dette vil gjelde også for strpl. § 216 b, i det regelen i strpl. § 216 a er gitt tilsvarende anvendelse jamfør første ledd annet punktum i strpl. § 216 b.

Etter de begrensninger som bestemmelsenes første ledd litra a) setter, er kontroll uaktuelt for svært mange alvorlige kriminelle handlinger. Lovgiver har imidlertid ment at det både er nødvendig og forsvarlig at man også utenfor disse tilfellene skal kunne iverksette kommunikasjonskontroll i forhold til alvorlig kriminelle handlinger.[49] I første ledd litra b) har man derfor utvidet adgangen til også å gjelde kriminelle handlinger med maksimumstrafferamme under lovens krav.

Inntil lovendringen 5. august 2005, inneholdt første ledd litra b) i begge bestemmelsene en en hoc-henvisning til straffeloven kapittel 8 og 9. Lovteknisk var dette enkelt da alle bestemmelsene i kapitlene automatisk tilfredstilte kriminalitetskravet i strpl. kapittel 16 a. I dag er anvendelsesområdet betydelig innskrenket, og en hoc-henvisningen er fjernet. De enkelte bestemmelsene i strl. kapittel 8 og 9 som har strafferamme under 10 og 5 år, men der det likevel skal være adgang til å kontrollere kommunikasjonen, er nå særskilt nevnt i bestemmelsene. Bakgrunn for endringen var Lundutvalgets utredning om straffelovens regler om rikets sikkerhet, og de etterforskningsmetoder som er aktuelle for saker om terrorisme.[50]

Etter strpl. §§ 216 a og 216 b begge bestemmelsenes første ledd litra b), kan handlinger etter strl. § 90 (om avsløring av hemmelige opplysninger om rikets sikkerhet), § 91 (om å sette seg eller andre i besittelse av opplysninger som nevnt i § 90), § 91 a (om innsamling av politisk eller personlig informasjon til fordel for fremmed stat ved hjelp av hemmelig innsamling eller ved bruk av ulovlige midler) og § 94 jf § 90 (om forbud mot å inngå forbund for å avsløre hemmelige opplysninger om rikets sikkerhet) gi adgang til kontroll,

[49] Se Ot.prp. nr. 64 (1998-99) punkt 8.3.2

[50] NOU 2003: 18 Rikets sikkerhet, side 147 avsnitt 8.4.3.3

herunder identifikasjon av kommunikasjonsanlegg. Straffeprosessloven gir § 216 a første ledd litra b) adgang til kontroll også etter § 104 a første ledd annet punktum (om dannelse, deltakelse eller rekruttering til organisasjon av militær karakter som har adgang til forråd av våpen og sprengstoff eventuelt at dens medlemmer har det, som har medlemmer under 18 år og som bruker personer under 18 år i fiendtlig aktivitet, eller andre skjerpende omstendigheter) og § 104 a annet ledd (om dannelse, deltakelse eller rekruttering til organisasjon som beskrevet under § 104 a første ledd annet punktum, eller andre sammenslutninger som har til formål å forstyrre samfunnsorden eller oppnå innflytelse i offentlige anliggender ved hjelp av forskjellige ulovlige midler).

I tillegg til bestemmelser i strl. kapittel 8 og 9, er det også andre bestemmelser i straffeloven med maksimumstrafferamme under lovens krav som kan gi adgang til kontroll etter strpl. §§ 216 a og 216 b begge bestemmelsenes første ledd litra b). Etter strpl. § 216 a gjelder dette strl. § 162 om narkotikaforbrytelser (gjelder ikke bruk og besittelse etter legemiddelloven § 31 annet ledd jf § 24 jf § 22)og § 317 jf § 162 (om heleri og hvitvasking i forbindelse med utbytte fra straffbare handlinger, narkotikaforbrytelser).[51] Det samme gjelder for handlinger som straffes etter § 5 i lov om kontroll med eksport av strategiske varer, tjenester og teknologi, blant annet utførsel av varer, tjenester og teknologi i strid med loven, meddelelse av uriktige opplysninger i forbindelse med utførsel eller overtredelse av vilkår loven har satt.[52]

Straffeprosessloven § 216 b første ledd litra b) gir i tillegg strl. § 145 annet ledd (om å skaffe seg uberettiget adgang til lagret eller overførbar data eller programutrustning), § 162 c (om å inngå avtale (”forbund”) med noen for å begå handling som kan straffes med fengsel i 3 år, dette som ledd i virksomheten til en kriminell organisasjon), § 204 første ledd litra d) (om barnepornografi), § 317 jf § 162 (se avsnittet ovenfor om oppregningen av bestemmelser etter § 216 a), og § 390 a (om forseelse mot en annens fred ved å opptre skremmende, besværlig eller ved annen hensynsløs atferd).

[51] Lov 4. desember 1992 nr. 132

[52] Lov 18. desember 1987 nr. 93

I forbindelse med oppramsingen i strpl. § 216 b første ledd litra b), kan man bli i tvil hvorvidt strl. § 390 a alene vil kunne gi adgang til identifikasjon og annen kontroll. Dette ut fra bestemmelsens utforming;
"som rammes av straffeloven §§ … 317, jf. §§ 162 eller 390 a." Dette kan vanskelig tolkes annerledes enn at strl. § 390 har selvstendig betydning, og kan gi adgang til kontroll uavhengig av andre bestemmelser. Heleri i forbindelse med forstyrring av en annens fred er upraktisk. Tolkningen har støtte i Ot.prp. nr. 64 (1998-99), " [v]ed telefonsjikane benyttes alltid telekommunikasjonsanlegg. Dermed vil det alltid foreligge trafikkdata fra selve lovbruddet. Også hacking skjer gjerne ved bruk av kommunikasjonsanlegg og etterlater seg dermed trafikkdata. … Departementet mener derfor at straffeloven §§ … 390a bør omfattes."[53]

2.1.8 Forholdet til utilregnelighet

Etter straffeloven kan ilagt straff bortfalle på bakgrunn av ulike omstendigheter.[54] Strl. § 44 bestemmer at dersom en person i gjerningsøyeblikket var psykotisk, bevisstløs eller var psykisk utviklingshemmet i høy grad, kan straff ikke idømmes. Psykotisk vurderes etter det medisinske prinsipp, noe som gjør den medisinske diagnose avgjørende. For begrepet "bevisstløs" gjelder at det finnes to former, nemlig absolutt og relativ. Med relativ bevisstløshet menes eksempelvis hypnose og søvngjengeri. Når det gjelder høy grad av psykisk utviklingshemming, går det en veiledende grense ved IQ 55.

Straffeloven § 46 bestemmer at ingen kan straffes for handling foretatt før fylte 15 år. (Ansvar inntrer fra og med fødselsdagen.) Både strpl. §§ 216a og 216b bestemmer at selv om straff ikke kan ilegges på grunn av strl. §§ 44 og 46, kan det besluttes at kommunikasjonskontroll, herunder identifikasjon skal iverksettes. For kontroll av kommunikasjonsmidler spiller det altså ingen rolle om det er utvist skyld eller ikke. Dette

[53] Ot.prp. nr. 64 (1998-99) kapittel 8.3.3.4 avsnitt 20

[54] Eskeland 2000 side 317-321

fremkommer også av strpl. § 216 a annet ledd annet punktum, som er gitt tilsvarende anvendelse for strpl. § 216 b i bestemmelsens første ledd annet punktum.

2.2 Begrepet identifisering

Etter gjeldende rett er det to måter å identifisere på; enten ved hjelp av temporær avlytting som vil bli behandlet i 2.2.1, eller sammenligning av data over tid som vil bli behandlet i 2.2.2.

2.2.1 Temporær masseavlytting jf strpl. § 216 a tredje ledd annet punktum

Straffeprosessloven § 216 a tredje ledd annet punktum har åpnet for at en ved hjelp av tekniske hjelpemidler, på en rask måte kan identifisere det kommunikasjonsanlegg som den mistenkte benytter. I dag finnes det en rekke slike hjelpemidler, som består av peileutstyr jf. *"teknisk utstyr"* i lovteksten. Selve identifiseringen skjer ved at peileutstyret blir rettet mot det området en vet mistenkte oppholder seg i. Dersom den mistenkte har en telefon, vil GSM-identifiseringssystemet fange opp strømmen av signaler som blir sendt fra hans telefon. Ulempen ved dette er at peileutstyret fanger opp alle telefonene i ett område, slik at også uskyldige tredjemenn kan risikere å bli avlyttet og identifisert. Ut fra strømmen av informasjon kan identifiseringssystemet identifisere hvilken telefon som ringer, hvilken telefon som blir opp ringt og innholdet i samtalen. Også andre kommunikasjonsanlegg identifiseres ved hjelp av teknisk utstyr og peiling, eksempelvis fasttelefon, telefaks og datamaskin.

Når det gjelder temporær avlytting, så er det som nevnt en fare for at også andre enn mistenkte kan bli avlyttet. Dette vil for eksempel være tilfellet der området mistenkte befinner seg i er en boligblokk, en større arbeidsplass eller en annen møteplass, der det kan befinne seg andre som også benytter et kommunikasjonsanlegg eksempelvis mobiltelefon.[55] Som nevnt ovenfor er det mulig å avlytte samtaler ved bruk av peileutstyret.

[55] Ot.prp. nr. 60 (2004-2005) punkt 8.1 side 104

Avlytting vil ikke alltid være nødvendig, men ofte vil det å høre stemmene være avgjørende for identifiseringen. Særlig er dette praktisk der avlyttingen skjer fra utsiden av bygningen og man ikke har mulighet til å vite hvilken telefon man for øyeblikket peiler. Det er forutsatt i forarbeidene at avlyttingen skal avbrytes med en gang det er klart at den avlyttede ikke har noe med mistenkte å gjøre eller saken for øvrig.[56] Det er imidlertid klart at selv om en tar alle mulige forholdsregler, vil utenforstående kunne bli avlyttet i kortere perioder.

Det er en forutsetning for adgangen til temporær masseavlytting at det kun er kommunikasjonsanlegg som ikke lar seg identifisere på annen måte, som kan være gjenstand for identifisering etter disse reglene. Det følger av kravet til vesentlighet i strpl. § 216 c første ledd som bestemmer at avlyttingen må være av vesentlig betydning for oppklaring av saken, og at oppklaringen ellers ville blitt vesentlig vanskeliggjort. Det er også en forutsetning at det foreligger særlige grunner etter strpl. § 216 c tredje ledd. Dette som en ekstra rettssikkerhetsgaranti for de uskyldige tredjemenn som blir fanget opp under avlyttingen. Selv om avlyttingen er forutsatt kun å foregå i en kortere periode. Strpl. § 216 c vil bli behandlet nærmere i avsnitt 2.3.

2.2.2 Peiling og sammenligning av data over tid jf strpl. § 216 b annet ledd litra c)

Mobiltelefoner lar seg som regel identifisere uten masseavlytting. Ot.prp. nr. 60 (2004-2005) forutsetter at også andre kommunikasjonsanlegg kan identifiseres på denne måten. Men dette vil være noe upraktisk for de kommunikasjonsanlegg som eksisterer i dag. Det anses som lite trolig at noen tar fasttelefonen eller telefaksen med seg når de forlater hjemmet, uansett om avstanden er så kort at trådløse telefoner fungerer. Denne identifiseringsmetoden er også upraktisk for datamaskiner som er koblet på nett, selv om det benyttes trådløst nettverk. Som sagt ovenfor følger en IP-adresse nettilgangen, og ikke den enkelte pc.

---

[56] Ot.prp. nr. 60 (2004-2005) punkt 8.5.3 side 111

Når identifisering skjer etter strpl. § 216 b annet ledd litra c), gjennomfører politiet tekniske observasjoner av anlegget for å kartlegge påloggede identiteter i et bestemt område. Observasjonene blir så sammenlignet med andre observasjoner gjort i annet område, slik at man ut fra dette kan se hvilke to identiteter som går igjen på de forskjellige stedene. Observasjonene blir gjort på steder politiet vet at den mistenkte oppholder seg på bestemte tidspunkter.[57] Ordet "*vet*" tyder på at politiet allerede må ha spanet på, eller på annen måte ha ervervet informasjon om mistenkte. Når sammenligningen er foretatt vil politiet normalt være i stand til å identifisere mistenkte. En kan likevel ikke se bort i fra at det i enkelte tilfeller skjer feil, slik at personer uten tilknytning til mistenkte eller saken forøvrig blir identifisert.

Observasjonene blir gjort ved å rette peileutstyr mot et nærmere bestemt område. I så måte er det lite som skiller identifisering etter strpl. § 216 b fra masseavlytting etter § 216 a. Forskjellen viser seg imidlertid ved tidsaspektet, ved at identifisering etter § 216 b vil ta noe lengre tid enn identifisering ved masseavlytting. I tillegg kommer at identifisering etter § 216 b vil virke langt mindre inngripende for uskyldige tredjemenn, selv om politiet skulle identifisere dem gjennom peilingen. Selve innholdet i kommunikasjonen har ikke blitt avslørt. Det er likevel krav om at identifiseringen må være av vesentlig betydning for oppklaringen av saken, og at oppklaring ellers ville blitt vanskeliggjort, se nedenfor under 2.3.2.

2.3 Tilleggskrav etter strpl. § 216 c

2.3.1 Indikasjonskrav

Etter strpl. § 216 c første ledd er det krav om at *"[t]illatelse til kommunikasjonskontroll kan bare gis dersom det kan antas at slik avlytting eller kontroll vil være av vesentlig betydning for å oppklare saken, og at oppklaring ellers i vesentlig grad vil bli vanskeliggjort."* Ordene "*må antas*" indikerer at det må foreligge mer enn en ren

[57] Se Ot.prp. nr. 60 (2004-2005) punkt 8.5.2 side 109.

formodning om at inngrepet vil fremskaffe opplysninger av vesentlig verdi, og om at etterforskningen ellers i vesentlig grad vil bli vanskeliggjort. Antakelsen må bygge på objektive kriterier som gir grunnlag for en viss grad av sannsynlighet. Det er enighet i juridisk teori at det neppe kreves sannsynlighetsovervekt.[58] Begrepet "*antas*" bør forstås på samme måte som i strpl. § 216 a tredje ledd første punktum, se 2.1.2 over. Etter min mening kan det kan diskuteres om det ikke bør kreves sannsynlighetsovervekt av hensyn til de uskyldige tredjemenn som blir berørt. Jeg går imidlertid ikke nærmere inn på denne debatten.

2.3.2 Vesentlighetskravet

Vesentlighetskravet består av to deler. For det første må identifiseringen være av vesentlig betydning for oppklaring av saken. Og for det andre må oppklaringen av saken bli vesentlig vanskeliggjort dersom det ikke iverksettes identifisering. Bjerke 2001 B. 1 sier at spørsmålet om betydning og vanskeliggjøring i praksis vil gå ut på ett.[59] Hensikten med regelen må være at kommunikasjonskontroll kun skal brukes der andre og mindre inngripende etterforskningsmetoder kommer til kort. Det følger av Ot.prp. nr. 10 (1976-77) side 6, at det stilles krav til konkret nødvendighet. Vesentlighetskravet er derfor et subsidiaritetskrav. Retten må også kunne se på hvorvidt det er fornuftig ressursbruk å iverksette kontroll ved vurderingen av om tillatelse skal gis. Det kreves likevel ikke at andre mindre inngripende metoder har vært forsøkt, det er nok at politiet har vurdert metodene og funnet de uegnet.

Kravet til vesentlighet i strpl. § 216 c første ledd gjelder kommunikasjonskontroll generelt, slik at det både omfatter avlytting etter strpl. §§ 216 a tredje ledd og annen kontroll etter 216 b annet ledd.

---

[58] Se for eksempel Bjerke 2001 B. 1, side 748

[59] Se Bjerke og Keiserud 2001 B. 1, side 748

2.3.3 Krav til særlig grunn

I henhold til strpl. § 216 c tredje ledd første punktum jf. annet ledd er det et krav til *"særlig grunn"* dersom identifisering skal iverksettes ved hjelp av masseavlytting. Kravet til "*særlig grunn*" gjelder ikke for identifikasjon etter strpl. § 216 b annet ledd bokstav c, peiling og sammenligning av data over tid. Begrunnelsen for at det ved masseavlytting gjelder et unntaksfritt krav til særlig grunn, er etter forarbeidene at det er vanskelig å mene noe kvalifisert om hvilke telefoner som vil bli avlyttet. Ved denne typen identifisering blir et helt område avlyttet, og det vil være vanskelig for politiet å unngå å fange opp andre telefoner. Kravet gjelder uansett om telefonen ikke er tilgjengelig for et stort antall personer, og selv om telefonen ikke tilhører en person i gruppen med særlig streng taushetsplikt jf. strl. § 144, jf. strpl. § 216 c annet ledd annet og tredje punktum.[60] Da det "vil være hovedregelen snarere enn unntaket at kontrollen vil fange opp telefoner som disponeres av personer utenfor den mistenktes krets, er departementet kommet til at kravet om særlige grunner bør gjelde generelt ved all masseavlytting, og ikke bare i situasjoner hvor politiet kan komme til å fange opp samtaler som føres på slike anlegg som nevnt i straffeprosessloven § 216 c annet ledd. Etter departementets syn taler personvernhensyn for en slik løsning, selv om masseavlyttingen som regel kun vil finne sted over en kort periode." [61]

Ved identifisering etter strpl. § 216 b gjør ikke de samme hensynene seg gjeldende. Kommunikasjonen blir ikke avlyttet i snever forstand, men kun sammenlignet med andre signalstrømmer i et annet område. Selve innholdet i kommunikasjonen blir ikke kjent. Det er derfor ikke så inngripende for de som blir utsatt for denne typen identifikasjon.[62]

Kravet til "*særlig grunn*" må forstås slik at det skal mer til her enn ellers, for å tillate bruk av identifisering. De grunnene som taler for identifisering må gjøre seg gjeldende med

---

[60] For nærmere behandling om strpl. § 216 c generelt, se for eksempel Andenæs 2000 B. 2 side 203, eller Bjerke og Keiserud 2001 B. 1 side 748-749.

[61] Ot.prp. nr. 60 (2004-2005) punkt 8.5.3 side 111, annen spalte

[62] Ot.prp. nr. 60 (2004-2005) punkt 8.5.2 side 110

særlig tyngde. Identifiseringen skal ikke utgjøre et uforholdsmessig stort inngrep i forhold til det som oppnås. Bestemmelsen gir derfor uttrykk av å være et særlig strengt forholdsmessighetsprinsipp, se 2.4 om strpl. § 170 a.

Det er flere momenter i vurderingen av om det foreligger særlige grunner. Et eksempel er den kriminelle handlings alvorlighetsgrad. Selv om de opplistede forbrytelsene i strpl. § 216 a alle er alvorlige, vil særlige grunner lettere sies å foreligge der det er snakk om en handling som er av de mer alvorlige. Det vil også være av betydning om masseavlytting er den eneste etterforskningsmetoden som kan antas å gi resultater. Det bør også tas hensyn til at forarbeidene forutsetter at kontrollen kun skal foregå over kort tid, og at kontroll skal avsluttes med en gang det er klart at samtalepartene ikke har noe med etterforskningen å gjøre. Poenget med identifiseringen er å skaffe identiteten til anlegget for så å kunne begjære ordinær avlytting. Departementet mener derfor at det gjennomgående bør stilles noe mindre krav til vurderingen i forbindelse med masseavlytting enn det gjøres i forhold til ordinær avlytting.[63]

Dersom det er grunn til å tro at etterforskningen vil bli vesentlig vanskeliggjort hvis ikke masseavlytting iverksettes, vil som regel kravet til særlig grunn være oppfylt. Vurderingen i forbindelse med denne type avlytting vil være preget av tidsaspektet. Dette kan tolkes som om kravet til særlige grunner lettere vil være oppfylt. Dette må imidlertid veies opp mot det forhold at masseavlytting vil berøre langt flere enn bare mistenkte, noe som igjen taler for en streng vurdering. Ved masseavlytting er det i tillegg stor fare for at enkelte av de telefoner som vil bli avlyttet tilhører personer i taushetsplikt-gruppen. Dersom kravet er for strengt vil kriminelle kunne innrette seg etter det, for eksempel ved å oppholde seg i et område der en lege holder til, og man vil ikke kunne få anledning til å iverksette kommunikasjonskontroll.

[63] Ot.prp. nr. 60 (2004-2005) punkt 8.5.3 side 111 annen spalte.

2.4 Krav til forholdsmessighet jf strpl. § 170 a

"Et tvangsmiddel kan brukes bare når det er tilstrekkelig grunn til det. Tvangsmidlet kan ikke brukes når det etter sakens art og forholdene ellers ville være et uforholdsmessig inngrep." Bestemmelsen setter begrensninger for adgangen til å iverksette kontroll av anlegg. Det må vurderes hvorvidt kontroll er ønskelig og hensiktsmessig på avgjørelsestidspunktet. Kontrollen må ikke utgjøre et uforholdsmessig inngrep. Retten må også vurdere om det finnes andre tiltak som kan anses tilstrekkelige. Temaet for vurderingen er "sakens art og forholdene ellers". Aktuelt i denne vurderingen vil være sakens mer eller mindre alvorlige karakter jf. kriminalitetskravet behandlet over i 2.1.7, og hvor sterk mistanken er. Videre hvor inngripende det vil være for mistenkte, og ikke minst for uskyldige tredjemenn som blir avlyttet og identifisert, og hvor lenge kontrollen er ment å vare. Det vil også være av betydning hvor vesentlig det er for etterforskningen at tiltak om kontroll blir iverksatt. Det bør tas hensyn til mistenktes personlige og sosiale forhold, for eksempel mistenktes livssituasjon.[64] Hensynet til tredjemann vil ha størst vekt, da involverte i alvorlig kriminalitet ikke har krav på samme vern. Selv om kommunikasjonskontroll ikke vil være et uforholdsmessig stort inngrep, er det ikke sikkert at det er tilstrekkelig grunn til å iverksette slik identifisering. Etter dette er det klart at kravet til forholdsmessighet henger sammen med tilleggskravene i strpl. § 216 c som er behandlet over i 2.3. Men mens strpl. § 216 c fokuserer på politiets behov, retter forholdsmessighetsprinsippet i strpl. § 170 a seg i hovedsak mot den som blir utsatt for inngrepet.

Når det gjelder momentet om sakens alvorlighetsgrad, vil det alltid være snakk om alvorlige kriminelle handlinger ettersom kriminalitetskravet er så strengt. Og når det gjelder mistanke, stiller strpl. §§ 216 a og 216 b krav til skjellig grunn. Det er også et generelt krav om *"rimelig grunn"* for i det hele tatt å iverksette etterforskning jf. strpl. § 224. For politiet kan det være en vanskelig avveining hva de skal legge frem av bevis ved begjæringen om kontroll. Noe må de naturligvis legge frem for å bevise at

[64] Ot.prp. nr. 64 (1998-1999) punkt 3.4 om forholdsmessighetsprinsippet.

mistanken er saklig begrunnet. Men dersom de gir uttrykk for å ha mye bevis, vil det ikke være behov for å iverksette kommunikasjonskontroll, og dermed vil retten kunne avvise begjæringen etter en forholdsmessighetsavveining.

3 Forholdet til EMK art. 8

3.1 De vernede rettigheter etter EMK art. 8 første ledd

I EMK art. 8 fastslås retten til privatliv, retten til familieliv, retten til hjem og retten til korrespondanse i en og samme bestemmelse. Rettighetene har ikke samme virkefelt, men rettspraksis viser at det til tider kan være vanskelig å trekke noen skarp grense mellom rettighetene. Rettighetene er ikke absolutte, i det inngrep kan skje på nærmere bestemte vilkår. Unntakene fra hovedregelen om respekt for rettighetene vil bli behandlet i 3.2.

To av de fire rettighetene blir ikke behandlet i det videre, dette er retten til respekt for familieliv, og retten til respekt for hjem.[65] Ikke fordi disse er av mindre betydning enn de to andre, men fordi rettighetene går i en litt annen retning enn kommunikasjonskontroll. Kjernen for retten til familieliv er å få være i fred. Konvensjonspraksis går på omsorgsovertakelse, samt klargjøring av begrepet ”familie”. Retten til ”hjem” skal ikke tolkes for snevert, men begrepet omfatter i alle fall ens bolig. Tenkelige inngrep her vil være ransaking, overvåking med skult utstyr, utålelige forstyrrelser med mer.

3.1.1 Gjennomføringsplikt

Etter EMK art. 1 er Norge som kontraherende part forpliktet til å respektere rettighetene etter EMK. I dette ligger ikke bare et vern mot inngrep, både fra det offentlige og av private, men også at partene skal sikre rettighetene. Med sikring menes å treffe positive tiltak for å gjennomføre rettighetene i praksis. EMK art. 1 er imidlertid en generell

[65] For behandling av disse rettighetene, se Møse 2002 kapittel 8 eller Aall 2004 kapittel 11

bestemmelse som blir slukt av de enkelte rettighetene. Brudd på en rettighet innbærer derfor også brudd på art. 1. I EMK art. 8 kommer ikke dette like godt frem, men det er sikker rett at en også her må innfortolke en dobbel gjennomføringsplikt.[66]

3.1.2 Retten til privatliv

Uttrykket *"privatliv"* er meget vidt, og EMD har uttalt at uttrykket ikke kan defineres uttømmende.[67] Derimot er det sikkert at uttrykket i første rekke omfatter den fysiske integritet (vernet supplerer EMK art. 3 om tortur, umenneskelig og nedverdigende behandling eller straff). Men også seksuelle forhold, overvåkning og vern mot innsamling av informasjon omfattes. Herunder vern mot misbruk i offentlige registre. En er beskyttet mot direkte inngripen i privatlivet, men som nevnt ovenfor er det ikke bare den innerste private sfære som er beskyttet. I det videre er det kun vernet mot overvåkning som vil bli behandlet.[68]

Retten til respekt for *"privatliv"* omfatter retten til å få være i fred med hensyn til private forhold. Iverksettes kommunikasjonskontroll, blir denne retten krenket. Dette er fastslått i en rekke dommer avsagt av EMD, blant annet i Klass and others v. Germany og Malone v. the UK.[69] Klass-saken gjaldt 5 tyske statsborgere som mente de tyske reglene om hemmelig kontroll med post, brev og telekommunikasjon, var i strid med EMK art. 8. Domstolen fant at telefonsamtaler omfattes av EMK art. 8 (1) *"privatliv"* og *"korrespondanse"*. Malone-saken gjaldt en antikvitetshandler som hadde blitt utsatt for telefonavlytting. Han mente at avlyttingen og kontrollen utgjorde inngrep i retten til *"privatliv"* og *"korrespondanse"*. Domstolen gjentok det standpunkt som ble tatt i Klass-saken. Standpunktet er konsekvent lagt til grunn i senere avgjørelser. I en klagesak mot

---

[66] Norsk lovkommentar ved Møse note 1

[67] Uttalelsen er fra Niemitz v. Tyskland, A 251-B (1992) avsnitt 29. Saken gjaldt hvorvidt en utført ransaking på klagerens advokatkontor var i strid med retten til respekt for privatliv etter EMK art. 8.

[68] For generelt om rettigheten, se Aall 2004 side 170 flg.

[69] Klass and others v. Tyskland, A 28 (1978) avsnitt 41. Malone v. UK, A 82 (1984) avsnitt 64.

Norge for Kommisjonen, fant man at selve eksistensen av norske regler for kommunikasjonskontroll var inngrep i forhold til EMK art. 8 (1).[70] Det forelå likevel ikke krenkelse av EMK art. 8, da reglene samsvarte med de krav som stilles etter art. 8 annet ledd.

Vernet etter *"privatliv"* er sterkest når etterforskningsmetodene retter seg mot det private hjem. Hjem må her tolkes utvidende slik at også kontoradresse og hotellrom vil omfattes, dette ble slått fast i Niemitz-saken avsnitt 31. Etter PG and JH v. the UK avsnitt 57 er det klart at dersom en har innrettet seg på personlig samkvem, gjelder vernet også om personen befinner seg i det offentlige rom.[71] Vernet vil imidlertid avta dersom en oppfører seg på en måte i det offentlige rom som må forventes å bli iakttatt av andre mennesker.

I saken PG and JH v. the UK hadde politiet satt i verk romavlytting og hentet inn trafikkdata, som følge av rykter om et forestående væpnet ran. Tre menn ble tiltalt for planlegging av ran, men de nektet å avgi forklaring og ville heller ikke avgi stemmeprøve i forbindelse med romavlyttingen. Politiet fikk tillatelse til å installere skjult avlyttingsutstyr i klagernes celler, og til å montere avlyttingsutstyr på klærne til de tjenestemennene som var til stede da klagerne ble gjort kjent med siktelsene. EMD fant at staten hadde krenket art. 8 i forbindelse med monteringen av det hemmelige utstyret på politistasjonen. Både romavlyttingen og innhenting av trafikkdata var inngrep i retten til privatliv.

Avlytting av fasttelefon vil i de fleste tilfeller vil være et inngrep i forhold til rettighetene i art. 8 første ledd. Verken rettspraksis eller juridisk teori er klar i forhold til avlytting av andre kommunikasjonsanlegg enn telefon. I det følgende må det derfor vurderes nærmere hvorvidt avlytting av andre kommunikasjonsanlegg nyter vern etter EMK art. 8.

Når det gjelder mobiltelefoner, stiller disse i en særstilling. Samtalene føres fra en telefon, og skulle derfor være omfattet av vernet. En telefonsamtale er en privat affære, i

[70] X v. Norge (13564/88)

[71] PG and JH v. the United Kingdom, RJD 2001-IX side 195

utgangspunktet burde man derfor kunne belage seg på at samtalen er vernet uansett hvor man befinner seg i det samtalen blir ført. Når man prater i mobiltelefon på gata må man være forberedt på at noen kan komme til å høre hva en sier. Ut i fra det som er sagt i PG and JH v. the UK vil samtaler ført på offentlig sted, eksempelvis på venterom, lettere falle utenfor vernet fordi en her har innrettet seg på en måte som gjør at andre kan observere. Etter min mening må dette sees i lys av det faktum at konvensjonen skal tolkes dynamisk og i takt med samfunnsutviklingen. I dag er det anslagsvis et fåtall av Europas befolkning som ikke har tilgang på mobiltelefon. NOU 2004: 6 legger til grunn at det i konvensjonspraksis ser ut som om "lytting og avlytting av samtaler personer har med hverandre i fortrolighet, lettere vil falle inn under vernet i art. 8 enn iakttakelse."[72] Riktignok gjelder forarbeidet politimetoder i forebyggende øyemed, men da metodene er de samme som politimetodene etter strpl. kapittel 16 a, vil uttalelsen ha relevans. Etter dette må det være riktig å si at mobilsamtaler er vernet mot inngrep.

Jeg går nå over til å drøfte hvorvidt de norske reglene for identifisering av kommunikasjonsanlegg utgjør inngrep i rettighetene etter EMK art. 8 (1). Det synes ikke og finnes rettspraksis eller juridisk litteratur som går på akkurat dette. I tråd med de tolkningsprinsipper som er presentert ovenfor i 1.9.2, vil vurderingen videre bygge på formålsbetraktninger og generelle betraktninger ut i fra EMDs tidligere avgjørelser, samt reelle hensyn. Forarbeidene er kun subsidiære kilder, og EMKs forarbeider antas ikke å kunne bidra i særlig grad jf. siste avsnitt i 1.9.2. Forholdet mellom de nye reglene i strpl. kapittel 16 a og EMK art. 8 første ledd blir diskutert i Ot.prp. nr. 60 (2004-2005) side 22-24. Departementet vurderer hjemlene til å være "godt innenfor de rammer våre folkerettslige forpliktelser trekker opp", men tar ikke uttrykkelig standpunkt til om de nye norske inngrepshjemlene vil være inngrep i art. 8 (1) forstand. Men når departementet vurderer identifikasjonsreglene opp mot art. 8 (2), kan det se ut som om de forutsetter at identifikasjon utgjør inngrep i rettighetene etter art. 8 (1). Dette har størst relevans i forhold til statenes skjønnsmargin som blir behandlet under i 3.2.3.

[72] NOU 2004: 6 Mellom effektivitet og personvern, punkt 4.3.5.2 side 37

EMD synes generelt å vektlegge hvorvidt det brukes tekniske innretninger og hjelpemidler ved avlyttingen av en telefon. Begge formene for identifisering krever bruk av teknisk utstyr. Identifisering vil gripe inn i uskyldige tredjemenns private sfære, spesielt ved masseavlytting. Dette gjelder selv om det kreves særlig grunn etter strpl. § 216 c, se 2.3.3, og tiltaket er forutsatt å vare kun kort tid. Det er som nevnt ovenfor forutsatt at avlytting skal avsluttes med en gang det er klart at vedkommende ikke har noe med saken å gjøre. Det kan ikke være tvil om at avlytting av uskyldige tredjemenn er inngrep i privatlivet etter EMK art. 8 første ledd.

Også i forhold til den mistenkte vil identifisering utgjøre et inngrep i vernet etter EMK art. 8. Det kan ikke være forskjell på avlytting etter at telefonen er entydig identifisert, og avlytting før identifikasjon er fullført. For den som blir avlyttet har det samme innvirkning, selv om avlytting som ledd i identifisering ikke er ment å foregå over lang tid. EMD synes å vektlegge personens egne forhold, og uttaler i Lüdi v. Sveits at dersom man driver kriminell virksomhet, må man regne med å komme innenfor politiets søkelys.[73] Likevel mener EMD i samme dom at telefonavlytting er inngrep i privatlivet.

Når det gjelder identifisering ved hjelp av peiling og sammenligning av data over tid, vil dette stå i en litt annen stilling enn masseavlytting. Dette fordi tiltaket ikke er fullt så inngripende. Politiet hører ikke på samtalene, men ser kun på signalstrømmen. I tillegg vil feilidentifisering høre til sjeldenhetene, selv om det er en risiko for at uskyldige blir identifisert. Det faktum at personer blir kartlagt på denne måten, taler for at også denne metoden for identifisering er et inngrep i retten til respekt for privatlivet. Det vises også til det som er sagt ovenfor om politiets bruk av tekniske innretninger og hjelpemidler. Der

[73] Lüdi v. Sveits, A 238 (1992) avsnitt 40. Saken gjaldt en mann som på oppdrag skulle skaffe og selge et stort kvantum narkotika. En polititjenestemann tok under dekke av å være narkotikaselger, kontakt med tiltalte og ga uttrykk for at han kunne skaffe narkotikaen. Tiltalte mente hans rett til privatliv var krenket som følge av at det var blitt brukt en politiprovokatør i saken, og at det var blitt iverksatt telefonavlytting. EMD fant at art. 8 ikke var krenket.

politiet har tatt i bruk slike metoder, vil det være et moment som taler for inngrep. Det vil også være et moment hvorvidt det finnes kontrollmekanismer. Det vil være mer betryggende dersom en avgjørelse er tatt av en domstol, enn om det er en politimann som har besluttet kontrolltiltak iverksatt. Kontrollmekanismer og rettssikkerhetsgarantier kommer med tyngde inn i vurderingen under 3.2.3, men vil også være et relevant moment i vurderingen her.

I Norge er avgjørelsene objekt for domstolskontroll, uansett om de i første omgang er iverksatt på beslutning av politiet. Dette taler for at det ikke er inngrep. Etter PG and JH v. the UK er det klart at innhenting av trafikkdata er inngrep i retten til privatliv eller korrespondanse, se dommens avsnitt 42.[74] Det følger av Peck v. the UK at identifikasjon som følge av fotografier tatt i unormale eller ydmykende situasjoner også er inngrep i privatlivet.[75] Det er ikke avklart om identifisering i normale situasjoner kan utgjøre et inngrep. Det er uansett klart at ens identitet er vernet etter art. 8 (1), og at statene har et overordnet ansvar for å sikre rettighetene, jf. også formålet med menneskerettighetene og EMK art. 1.

Når trafikkdata og fotografier er inngrep, kan det diskuteres hvor den nedre terskel for inngrep ligger. Felles for disse inngrepene er at man har et klart bilde av hvem det er som får sitt privatliv krenket. Etter en peiling i forbindelse med identifisering, sitter politiet igjen med en rekke nummer, de har ikke informasjon om identiteten til den som har blitt peilet. Teletilbyder er ikke pliktig til å utlevere taushetsbelagte opplysninger om abonnementet etter ekoml. § 2-9, da nettopp en slik situasjon vil kunne være et særlig

---

[74] Trafikkdata kan begjæres utlevert etter strpl. § 216 b annet ledd litra d). I henhold til bestemmelsen kan politiet innhente historiske og fremtidige opplysninger om hvilke kommunikasjonsanlegg som har vært, eller skal settes i forbindelse med anlegg som er under kontroll.

[75](2003) 36 EHRR 41 side 719. Klageren ble filmet av et overvåkingskamera i det han prøvde å begå selvmord med en kjøkkenkniv. Politiet ble varslet og fikk avverget forsøket. Bildene fra overvåkingskameraet ble senere vist frem i media i en rekke tilfeller for å vise overvåkingssystemets effektivitet. EMD fant brudd på art. 8.

forhold som gjør det utilrådelig å gi ut opplysninger. Se ovenfor under 1.8. Etter sammenligningen, vil politiet derimot kunne få utlevert opplysninger, som følge av at mistanken knytter seg til et bestemt identifisert kommunikasjonsanlegg.

I PG and JH v. the UK uttaler EMD i avsnitt 57 "[t]he Court has referred in this context to the Council of Europe's Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data, which came into force on 1 October 1985, whose purpose is "to secure in the territory of each Party for every individual ... respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to the automatic processing of personal data relating to him" (Article 1), such data being defined as "any information relating to an identified or identifiable individual"(Article 2)". Domstolen viser til at det er av betydning om informasjon blir lagret systematisk eller permanent i registre, og at det derfor vil være inngrep i retten til privatliv dersom sikkerhetsvakter skaffer informasjon om en person, uansett hvilken metode som benyttes.

Det følger av strpl. § 216 g at overskuddsinformasjon skal tilintetgjøres snarest mulig. Data som ikke samsvarer med data fra annen peiling, vil være overskuddsinformasjon og dermed bli slettet. Dette er en rettssikkerhetsgaranti for den som blir peilet. Det må skilles mellom informasjon som samles inn av sikkerhetsvakt, og informasjon som politiet innhenter. Når politiet skaffer seg slik informasjon er det fordi de har sterke grunner til det. Informasjon som sikkerhetsvakter skaffer seg, som i tilfellet i den refererte saken, er ikke hjemlet i streng lovgivning. Det må derfor stilles strengere krav til anskaffelse av slik informasjon.

Med utgangspunkt i de generelle betraktningene som er presentert her, er jeg under tvil kommet til at selve peilingen og sammenligningen av data ikke utgjør et inngrep i vernet etter art. 8. For en tredjeperson vil det kanskje føles inngripende å bli peilet, men politiet kan ikke benytte dataen til noe. Annerledes vil det være for mistenkte, og eventuelle andre personer som mer eller mindre tilfeldig befinner seg i nærheten av han i de ulike områdene, og som følge av dette blir identifisert. Både for de uskyldige tredjemenn og mistenkte, vil

dette føles særlig inngripende. På bakgrunn av drøftelsen over må identifisering av personer også ved hjelp av denne metoden være et inngrep i retten til privatliv.

3.1.3 Retten til korrespondanse

Begrepet korrespondanse må forstås vidt. Dette fremgår av dommene beskrevet over i 3.1.2 som også ble forankret i retten til korrespondanse. Det er vanskelig å skille mellom de to rettighetene, da de langt på vei flyter over i hverandre. Se Domstolens uttalelse ovenfor i Niemitz-saken om at privatliv ikke kan defineres uttømmende. Retten innebærer både muntlige og skriftlige meddelelser. Det er private meddelelser som vernes, i motsetning til informasjon av mer generell karakter som vernes av EMK art. 10. Korrespondanse dreier seg om kommunikasjon, typisk ved hjelp av telefon, brev eller e-post.[76] Straffeprosessloven gir hjemmel til forskjellige drastiske inngrep, som å avlytte, innstille, avbryte, stenge, innhente trafikkdata og identifisere anlegg. I avsnittet om "retten til privatliv", har kommunikasjonsanlegget telefon blitt vurdert mot EMK art. 8. Objektet for vurdering i dette kapittelet vil være hvorvidt kontroll av telefaks og datamaskin kan sies å utgjøre et inngrep i retten til korrespondanse. Når disse kommunikasjonsanleggene behandles her, er det fordi kommunikasjon gjennom disse anleggene lettere vil falle inn under begrepet korrespondanse.

En stor del av rettspraksis på dette området omhandler fangers rett til korrespondanse. Det er fastslått at frihetsberøvelse som sådan ikke automatisk gir rett til kontroll av fangers korrespondanse. En viss form for kontroll er derimot påkrevd. Fengselsmyndighetene kan åpne post dersom de mener at posten kan ha ulovlig innhold som ikke har kommet til syne ved annen undersøkelse. Dette ble slått fast i Campbell v. the UK.[77] Saken gjaldt en fange som hadde fått åpnet og lest sine brev til og fra advokat og Kommisjonen. Han mente at åpningen og lesingen av hans post var et inngrep etter EMK art. 8 (1). Domstolen var enig i dette, og uttaler i avsnitt 48 at dette gjelder uansett innhold. Korrespondanse mellom klient

[76] For generelt om rettigheten, se Aall 2004 side 193 flg.

[77] Campbell v. the United Kingdom A 233 (1992)

og advokat vil alltid være av privat og konfidensiell natur, og man kan vanskelig skille mellom brev som gjelder klientens sak eller brev som gjelder andre ting, eksempelvis klage på fengselsmyndighet. Det fremgår av dommen at det kun i unntakstilfeller vil være lovlig å lese brev fra advokat til innsatt klient, nemlig der man frykter misbruk som kan sette fengselet eller andre i fare.

Campbell-saken går direkte på brevkontroll, men man må kunne legge til grunn at dette gjelder generelt, slik at kontroll av kommunikasjon som personer har med hverandre på fortrolig vis, lettere vil være vernet etter EMK art. 8 (1). Særlig gjelder det der personene har innrettet seg på privat samkvem, for eksempel e-post.

I vurderingen hvorvidt et kontrolltiltak utgjør et inngrep i retten til korrespondanse, tar EMD utgangspunkt i de vurderingselementer som er nevnt ovenfor under drøftelsen av retten til privatliv. Herunder blant annet formålsbetraktninger. Formålet med konvensjonen er å sikre individene de rettigheter som er fastlagt i konvensjonen. Det kan ikke være tvil om at både telefakser og e-poster er former for korrespondanse som nyter vern etter EMK art. 8 (1). Det kan heller ikke være tvil etter drøftelsen over, at avlytting og annen form for kontroll er inngrep i rettigheten. Drøftelsen i det videre vil derfor konsentrere seg om hvorvidt de ulike former for identifisering av anleggene er i strid med art. 8.

Identifisering ved hjelp av peiling og sammenligning av data over tid, er nokså upraktisk i forhold til telefaks, fasttelefoner og datamaskiner, jf. 2.2.2. Etter min mening er det derfor ikke nødvendig å gå inn på en nærmere vurdering av hvorvidt denne metoden utgjør inngrep i retten til korrespondanse.

Ovenfor er det konkludert med at masseavlytting av telefonsamtaler er inngrep i retten til privatlivet. Blant annet på grunn av formålet med selve konvensjonen. Det er nevnt ovenfor i 1.9.2 under formålstolkning, at formålet med EMK blant annet er å sikre individenes rettigheter. Rettighetene må sees i lys av samfunnsutviklingen, slik at det vern rettighetene gir, utvikler seg i takt med utviklingen i samfunnet forøvrig. Dersom det ikke hadde vært

tilfelle hadde man kunnet utvikle teknologien og grepet inn i individenes private sfære, mens menneskerettighetene, som stod på stedet hvil, ikke hadde gitt vern mot inngrepet. Når masseavlytting nå er mulig, bør EMK gi vern også i disse tilfellene.

En må også ta i betraktning at politiet ikke vet hvem de overvåkede anleggene kommuniserer med. Dersom en av partene tilhører gruppen med streng taushetsplikt (se 2.3.3) vil kontrollen lettere utgjøre et inngrep. Lovgiver har også tatt høyde for at dette er et inngripende tiltak, i og med at det er et unntaksfritt krav til særlige grunner i forbindelse med iverksetting av masseavlytting. Videre taler det for inngrep at det benyttes tekniske hjelpemidler ved identifiseringen jf. drøftelsen over under retten til privatliv. Det taler mot inngrep at det finnes flere rettsikkerhetsgarantier for å beskytte individene mot masseavlytting. Blant annet at beslutning blir truffet av retten, at overskuddsinformasjon skal slettes, og at det finnes et utvalg som i ettertid vurderer de tillatelser til kontroll som er gitt.

Ut i fra selve formålet med konvensjonen og bestemmelsen forøvrig, vil masseavlytting utgjøre et inngrep i retten til korrespondanse, både i forhold til uskyldige tredjemenn og mistenkte selv. Hertil kommer at en ved kommunikasjon gjennom telefaks og datamaskin, fortrinnsvis e-post, har innrettet seg slik at andre ikke skal kunne få innsyn i kommunikasjonen. Det sees i denne sammenheng bort fra at både e-poster og telefakser kan bli feilsendt. Formålsbetraktninger, inngrepets styrke og hensynet til den enkelte borger må her veie tyngre enn kontrollmekanismer, slik at masseavlytting er inngrep i retten til korrespondanse.

3.2 Unntakene i EMK art. 8 annet ledd

Unntakene i art. 8 annet ledd er kumulative vilkår, noe som gjør at dersom et vilkår ikke er oppfylt, foreligger det krenkelse av hele artikkelen.

3.2.1 Lovkravet

Inngrepet må være i samsvar med loven.[78] Ordet lov må tolkes utvidende slik at det ikke kun omfatter formell lov. Men selv om dette er tilfellet, viser praksis at andre hjemler vanskelig vil tilfredsstille øvrige krav konvensjonen stiller til hjemmelsgrunnlaget. Alminnelig handlefrihet vil derfor ikke bli godtatt. Det ble slått fast i Sunday Times v. the UK at regler utviklet gjennom nasjonal rettspraksis, sedvane og administrativ praksis er alternative hjemler.[79] Saken gjaldt en engelsk avis som fikk trykkerestriksjoner i forbindelse med en artikkel. EMD fant at EMK art. 10 var krenket. Begrepet "lov" er autonomt, og dommen har derfor betydning også utenfor art. 10. Dette er også slått fast i Silver v. the UK.[80] Imidlertid fremkommer det av en rekke dommer, blant annet Sunday Times-saken avsnitt 49, at det stilles kvalitetskrav til lovene. Lovene skal være tilstrekkelig tilgjengelige og klare. Det er grunn til å merke seg at når EMD aksepterer uskreven rett som lov i forhold til Storbritannia, som bygger på commom law-systemet, er det ikke selvsagt at de ville godtatt det samme i forhold til Norge. Hjemmelen fremstår som atypisk fordi det norske legalitetsprinsippet krever formell lov.

Det er et hovedformål at rettstilstanden skal være forutberegnelig, men for at det skal la seg gjøre må loven være tilgjengelig. I dette ligger at loven må eksistere på handlingspunktet, jf. Grl. § 96 forbud mot lovers tilbakevirkende kraft. For regler som retter seg mot myndighetene, som reglene om kommunikasjonskontroll jo gjør, er dette begrunnet i hensynet til å forebygge vilkårlighet og myndighetsmisbruk. I forhold til individene er det krav om at reglene er kunngjorte. Det er ikke tilstrekkelig at de er vedtatte. Utgangspunktet om forutberegnelighet må modifiseres i forhold til hvilket tiltak det er tale om. I forbindelse med identifisering og annen avlytting, står tiltaket i veien for fullstendig forutberegnelighet. Dette fordi mistenkte da lettere vil kunne innrette seg på en slik måte at han unngikk

---

[78] I Aall 2004 kapittel 7 gis det en generell redegjørelse for lovkravet.

[79] A 30 (1979) avsnitt 47

[80] A 61 (1983) avsnitt 85. Saken gjaldt fangers rett til korrespondanse, og hvorvidt fengselsmyndighetenes kontroll av brev innebar krenkelse av art. 8.

kommunikasjonskontroll. Men når det er sagt, er det viktig at reglene er tilstrekkelig klare for å sikre rettssikkerheten gjennom kontrollmekanismer. Dette gjelder både den personelle, prosessuelle og materielle kompetanse.

Når det gjelder kravet til tilstrekkelig klarhet, stiller dette krav både til lovgiver og til rettsanvender. Lovgiver må utforme lovene tilstrekkelig presise, slik at man unngår vage formuleringer og utvidende tolkning. Rettsanvender må anvende loven i samsvar med naturlig forståelse av ordlyden. Likevel er det i Sunday Times-saken uttalt at statene har en viss skjønnsmargin når det gjelder utformingen av lov. Det må tas hensyn til at ikke alle områder lar seg regulere fullt ut, samtidig som man stadig er nødt til å ha samfunnsutviklingen i tankene. Til en viss grad vil det svekke forutberegneligheten dersom det til stadighet kommer ny lov fordi samfunnsutviklingen har gjort at den gamle lovteksten ikke lengre er anvendbar. Loven bør likevel utformes tilstrekkelig presis slik at individene kan forutberegne sin rettsstilling og innrette seg heretter. Det er klart at jo mer vidtgående inngrepet er, jo sterkere er kravet til presishet. EMD stiller strenge krav til klar lovhjemmel i forbindelse med kommunikasjonskontroll. I tillegg har Domstolen lagt vekt på fragmentering av reglene. I saken Kruslin v. France avsnitt 34 kom EMD til at det forelå krenkelse fordi reglene måtte utledes av en rekke kilder, noe som kunne underminere forutberegneligheten og tilgjengeligheten.[81]

Det kan ikke være tvilsomt at norsk formell lov er lov også i EMKs forstand. Avgjørende blir derfor om kvalitetskravene er oppfylt. Det må være klart at de norske reglene oppfyller kravet til presishet. De norske reglene gir ikke rom for mange tolkningsspørsmål, selv om enkelte av begrepene gir uttrykk for skjønnsmessige vurderinger som kan være vanskelig å forutberegne for den enkelte. De personelle og de prosessuelle kompetansereglene er samlet i ett kapittel i straffeprosessloven, noe som gjør det enkelt å finne frem. Samt at både strpl. §§ 216 a og 216 b oppstiller kriminalitetskravet på en ryddig måte, selv om de

[81] A- 176-A (1990). Saken gjaldt avlytting av klagerens telefon i forbindelse med at en mann som var under etterforskning bodde hos klageren. EMD konstaterte krenkelse av art. 8 da lovhjemmelen ikke satte tilstrekkelig klare rammer for telefonavlytting.

materielle bestemmelsene er regulert i straffelovgivningen. Begge lovene er lett tilgjengelige på lovdatas gratisside, samt at bibliotekene har Norges lover i boks form. Reglene er også kunngjorte i Norsk Lovtidende. Det må derfor konkluderes med at de norske reglene om identifikasjon samsvarer med lovkravet i EMK art. 8

3.2.2 Relevante formål

De formål som kan være legitime i forhold til inngrep i art. 8 er opplistet i bestemmelsens annet ledd. Blant annet er inngrep av *"hensyn til den nasjonale sikkerhet, offentlige trygghet…, for å forebygge uorden og kriminalitet,…, eller for å beskytte andres rettigheter og friheter"* legitime formål. I Klass and others-saken (se ovenfor) uttaler EMD at telefonavlytting kan begrunnes i slike hensyn som ovenfor (se avsnitt 44-46), men det vil avhenge av formålet med de nasjonale bestemmelsene. Når det etter norsk rett iverksettes identifikasjon av kommunikasjonsanlegg, er dette som ledd i etterforskningen av alvorlige kriminelle handlinger jf. 2.1.7 ovenfor. Formålet er å avdekke og oppklare straffbare forhold av en viss alvorlighet for å kunne gjøre straffansvar gjeldende. Det kan ikke være tvil om at etterforskning for å oppklare alvorlig kriminalitet vil være av hensyn til et eller flere av de ovenfor nevnte formål. Hvilket formål som vil være relevant, vil avhenge av hvilken handling det er som er begått.

3.2.3 Nødvendig i et demokratisk samfunn

Dersom et inngrep er i samsvar med lov, og inngrepets formål er i tråd med de legitime formål som oppstilles i art. 8, vil en eventuell krenkelse avhenge av om inngrepet er "*nødvendig i et demokratisk samfunn*". Nedenfor følger derfor en drøftelse av hvorvidt de norske reglene for identifisering av kommunikasjonsanlegg kan sies å være nødvendig.[82]

Det er ikke umiddelbart klart hva som menes med begrepet "*nødvendig*". Begrepet har vært gjenstand for vurdering i en rekke dommer, og i Handyside v. the UK ble begrepet forsøkt

[82] Møse 2002 gir en kort redegjørelse på side 99-100.

gitt et klarere innhold[83]. EMD uttalte der at begrepet ikke er synonymt med ordet ”uomgjengelig”, men det er heller ikke like fleksibelt som ”… such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable"”. I Olsson v. Sweden ble begrepet gitt et mer presist innhold; “the notion of necessity implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued; in determining whether an interference is "necessary in a democratic society", the Court will take into account that a margin of appreciation is left to the Contracting States.”[84]

Vurderingstemaet blir i det videre om de norske reglene kan sies å være et utslag av et presserende sosialt behov, og om inngrepet er proporsjonalt med de mål som søkes oppnådd. I vurderingen må det tas høyde for den kontraherende stats skjønnsmargin, men EMD uttaler i Silver and others v. the UK avsnitt 97 b) at det er opp til Domstolen i siste instans å avgjøre hvorvidt nasjonale regler samsvarer med konvensjonen. I denne forbindelse skriver Jørgen Aall i sin bok ”Rettergang og menneskerettigheter” side 55 at ”[h]vorvidt statens vurdering vil bli tilsidesatt, må forventes å avhenge av på den ene siden hvilke tungtveiende samfunnsinteresser som står på spill, og på den annen side hvilken rettighet som er berørt og hvor byrdefullt det er for staten å imøtekomme individets interesser i den foreliggende situasjon. Videre må det forventes at prøvingsintensiteten vil variere med hvor godt egnet forholdet er for internasjonal overprøving. Jo mer renskåret rettslig spørsmålet er, desto mer må det antas at EMD føler seg kallet til å foreta en selvstendig vurdering og avgjørelse. Det motsatte utgangspunkt vil være tilfelle i relasjon til fakta og skjønnsmessige vurderinger.”

Det kan diskuteres om “presserende sosialt behov” er mer nøyaktig enn “*nødvendig i et demokratisk samfunn*”. Begge uttrykkene er generelle og sier lite om vurderingstemaet.

---

[83] A 24 (1976) avsnitt 48-49, saken gjaldt hvorvidt et beslag og inndragning av bok med pornografisk og annet utfordrende innhold ment for skoleelever var en krenkelse av EMK art. 10.

[84] A 130 (1988) avsnitt 67, saken gjaldt hvorvidt omsorgsovertakelse av tre barn innebar en krenkelse av art. 8 retten til familieliv.

Likevel er jeg tilbøyelig til å mene at "presserende sosialt behov" gir flere føringer enn det "*nødvendig i et demokratisk samfunn*" gjør. Dette fordi ordet "presserende" gir assosiasjoner til noe som er tvingende nødvendig, altså strengere enn nødvendig. Langt på vei vil denne vurderingen gå over i forholdsmessighetsvurderingen i forhold til at dersom det finnes en etterforskningsmetode som er mindre inngripende, og som ville ha gitt resultat, vil inngrepet lettere være uforholdsmessig, og dermed heller ikke tvingende nødvendig.

Når det gjelder forholdsmessighetsvurderingen er det som sagt nødvendig at det er proporsjonalitet mellom de mål som søkes oppnådd, og de midler som tas i bruk for å nå målet.[85] Dette innebærer at hensynet til borgernes privatliv, og samfunnets behov for å kunne bruke tvangsmidler i bekjempelsen av alvorlig kriminalitet, må avveies mot hverandre. Det må tas hensyn til både mistenkte og de uskyldige tredjemenn som blir avlyttet som ledd i identifiseringen. I den forbindelse må en se på de rettssikkerhetsgarantier som er oppstilt i nasjonal lovgivning. Det følger av sitatet fra Silver-saken at det ikke er tilstrekkelig at tiltaket er ønskelig, men det kreves heller ikke at det er uunnværlig. EMD legger vekt på om mindre inngripende metoder kommer til kort. Når det gjelder statenes skjønnsmargin og de mest inngripende metodene, som romavlytting og telefonavlytting, har EMD for det meste bare overprøvd om hjemmelen i tilstrekkelig grad oppstiller rettssikkerhetsgarantier. Se Klass-saken avsnitt 50.

Etter norsk rett blir den konkrete anvendelsen av tvangsmidler prøvd etter regelen om forholdsmessighet i strpl. § 170 a, i tillegg til kravene til vesentlighet og indikasjon i 2.3. I forhold til masseavlytting stilles det også krav til særlige grunner jf. 2.3.3. Det er retten som avgjør hvorvidt begjæring om identifikasjon tas til følge, og som dermed vurderer om de materielle vilkårene for iverksetting av tiltak er tilstede. Kun i ytterste tilfelle vil påtalemyndigheten kunne iverksette hurtigkobling, men da må begjæring forelegges retten senere. Det er en betryggende garanti at avgjørelse er underlagt kontroll av jurister med

[85] Aall 2004 skriver på side 129 om forholdsmessighetskontroll etter EMK.

særlig kompetanse. I den forbindelse bør en huske at mistenkte får oppnevnt "hemmelig forsvarer" for å forsvare hans interesser under behandlingen av saken, se 1.6.

I tillegg til disse garantiene, stiller straffeprosessloven opp en del andre begrensninger for bruken av kontrolltiltak. Straffeprosessloven § 216 f setter grenser for hvor lenge politiet kan avlytte et kommunikasjonsanlegg. For selve identifiseringen er det en forutsetning at avlyttingen skal avsluttes straks man har fastslått mistenktes identitet. Tidsbegrensningen i strpl. § 216 f har derfor ikke betydning for denne delen av avlyttingen. For de som har blitt avlyttet eller peilet er det også viktig å vite at all overskuddsinformasjon skal tilintetgjøres snarest mulig etter strpl. § 216 g. Det er imidlertid gjort unntak for informasjon som fremkommer under avlytting som kan brukes i forebyggelsen eller etterforskningen av straffbare handlinger. Straffbare handlinger må her tolkes som et generelt begrep, som ikke viser tilbake på den konkrete handling som i første omgang gjorde at identifisering ble iverksatt.

I tillegg til at domstolen foretar prøving av begjæringen, finnes det et utvalg, Kontrollutvalget, som skal etterkontrollere skjult metodebruk.[86] Utvalgets formål er å foreta fortløpende kontroll med særlig vekt på enkeltindividets rettssikkerhet jf. loven § 2. Utvalget er et uavhengig forvaltningsorgan. Kontrollen går dels ut på at generell praksis blir gjennomgått, men også enkeltsaker blir vurdert. Man må derfor kunne si at rettssikkerheten er tilstrekkelig ivaretatt, i og med at det etter norsk rett kan sies å foreligge en dobbeltkontroll av de tvangsmidler som blir iverksatt. Det er imidlertid alltid fare for misbruk.

En annen rettssikkerhetsgaranti er at man på begjæring skal kunne få opplyst hvorvidt man har vært underlagt kontroll jf. strpl. § 216 j.[87] Dette utgangspunktet må modifiseres i det man bare kan få bekreftende svar, aldri avkreftende svar, på hvorvidt kontroll har vært

---

[86] Lov 3.februar 1995 nr. 7, lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste. For nærmere om kontrollutvalget, se Ot.prp. nr. 83 (1993-94) og NOU 1994:4.

[87] Også regulert i kommunikasjonskontrollforskriften §§ 20-24

iverksatt. Fra samme utgangspunkt er det gjort en rekke andre unntak, blant annet for saker om overtredelse av strl. kapittel 8 og 9 (en hoc-henvisningen er ikke fjernet her) om rikets sikkerhet. Det er også viktig å merke seg at underretning ikke kan gis før tidligst ett år etter at kontroll ble avsluttet.[88]

Når det etter norsk rett iverksettes identifisering, er det som sagt for å etterforske og oppklare alvorlige kriminelle handlinger. Tiltaket utgjør et ledd i beskyttelsen av rikets og enkeltindividets sikkerhet. EMD har påpekt flere ganger at konvensjonen er utformet for å opprettholde, og fremme, ideene og verdiene i et demokratisk samfunn. De presserende samfunnsmessige behov må derfor relateres til det legitime formål inngrepet skal ivareta. I vurderingen av hvilke av to onder en vil utsette borgeren for, må en ha i mente at identifisering ved hjelp av avlytting og peiling er en trussel mot personvernet til utenforstående. Kommunikasjonskontroll er et ekstraordinært etterforskningsmiddel som bryter sterkt med alminnelige personvernhensyn. Likevel er det viktig for den enkelte borger at staten tar ansvar ved å oppklare forbrytelser og straffe forbryterne. Det vises her til det som er skrevet ovenfor om nødvendigheten av hjemmelen til identifisering. Politiet har i mange tilfeller blitt hengende etter i etterforskningen fordi de ikke har kunnet entydig bestemme hvilken identitet kommunikasjonsanlegget har, og dermed heller ikke fått tillatelse til avlytting. Når de har klart å finne frem til riktig anlegg, har mistenkte for lengst et nytt anlegg. (Dette er mest praktisk for mobiltelefoner.) Det kan derfor konkluderes med at det er et tvingende sosialt behov for reglene.

Inngrepstyrken ved identifisering er forskjellig ettersom det er snakk om masseavlytting eller peiling og sammenligning av data over tid. Likevel er det ikke tvil om at det i begge tilfeller er snakk om inngripende tiltak. Det er klart at tiltakets art og karakter vil påvirke kravet til nødvendighet. Men som sagt, legger lovgiver til grunn at behovet for identifiseringshjemlene er stort. EMD uttaler i Dudgeon v. the UK at grunnene for å godta

[88] For nærmere behandling av reglene, se eksempelvis Bjerke 2001 B. 1 side 761-763

reglene må være relevante og tilstrekkelige.[89] Det kan ikke være tvil om at grunnene til å ha identifiseringshjemler er relevante. Avgjørende blir derfor om de er tilstrekkelige. Ot.prp. nr. 60 (2004-2005) kapittel 8 gir inntrykk av at denne måten å identifisere på er den eneste måten som er brukbar. Det er lagt til grunn at politiet også på andre måter vil kunne kartlegge identiteten på anleggene, men dette vil ta uforholdsmessig lang tid slik at det allerede kan være for sent.

Med de kontrollmekanismer og begrensinger som er inntatt i straffeprosessloven må det kunne sies at grunnene også er tilstrekkelige. Det skal en del til før det gis tillatelse til identifisering, og selv om det er inngripende både for mistenkte og uskyldige tredjemenn, må det kunne sies at deres rettssikkerhet er tilstrekkelig ivaretatt. Dog er metodene for identifisering meget inngripende, men når andre metoder er utilstrekkelige og man ikke kommer videre i etterforskningen uten identifisering, må det sies at målet, nemlig å oppklare og etterforske kriminalitet, er proporsjonalt med middelet. Dette vil kunne diskuteres dersom etterforskningen blir innstilt eller mistenkte (tiltalte) i en straffesak blir frifunnet, men igjen; mistankekravet gjør at kontroll ikke kan iverksettes uten at det er snakk om alvorlige handlinger.

I forhold til statens skjønnsmargin dreier det seg om særdeles viktige rettigheter, retten til privatliv og korrespondanse, og det er tungtveiende samfunnsinteresser som står på spill. Dette skulle tilsi at EMDs prøvingsintensitet er stor. Men som sagt ovenfor, EMD har i stor grad bare overprøvd hvorvidt det oppstilles gode nok rettssikkerhetsgarantier. Det er derfor grunn til å anta at Norges skjønnsmargin i dette tilfellet, ikke vil bli overprøvd i særlig grad. Ovenfor er det konkludert med at hjemlene er et utslag av et presserende sosialt behov, og at identifiseringen er proporsjonal med de mål som oppnås. Det må derfor konkluderes med at de norske reglene for identifisering er i samsvar med de krav som stilles etter EMK art. 8. EMD må imidlertid være overbevist om at inngrepet i det enkelte

[89] A 45 (1981) avsnitt 54, saken gjaldt hvorvidt reglene som gjorde homoseksuelle handlinger straffbare i Nord-Irland var i strid med art. 8. EMD fant at artikkelen var krenket i det belastningen som lovgivningen medførte var uforholdsmessig i lys av formålet med lovgivningen.

tilfelle var nødvendig tatt i betraktning faktum og omstendigheter som råder i den enkelte sak, slik at EMD ikke nødvendigvis vil konkludere med det samme.

4 Rettspolitisk vurdering av de norske reglene

De nye identifikasjonshjemlene har som formål å etablere bedre og effektive etterforskningsmetoder. Ved å utvide adgangen til bruk av kommunikasjonskontroll etter strpl. kapittel 16 a, håper man at flere alvorlige kriminelle handlinger vil bli oppklart. Dette vil i neste omgang føre til at flere skyldige blir dømt.

Identifisering er meget ressurskrevende, både personelt og materielt, men det er antatt at metodene vil gjøre at etterforskningen tar kortere tid. Dette vil føre til redusert saksbehandlingstid hos politiet i straffesaker, samtidig som arbeidsbelastningen til domstolene vil øke, både med hensyn til antall begjæringer og påkjæringer.

Det er vanskelig for meg å mene noe kvalifisert om hvor mye samfunnet økonomisk sparer på de nye lovhjemlene, men lovgiver har forutsatt at gevinsten er betydelig. Det blir også påpekt av flere høringsinstanser, at det brukes "uforholdsmessig mye tid på å identifisere GSM-telefoner og andre kommunikasjonsanlegg og at lovforslaget derfor vil kunne gi en betydelig effektiviseringsgevinst."[90]

Justiskomiteen uttaler at "[l]oven løfter vanskelige avveininger mellom personvern og hensynet til en effektiv kriminalitetsbekjempelse. Dette stiller store krav til den nærmere utformingen av loven. Komiteen mener det er viktig å komme frem til løsninger som balanserer samfunnets behov for å avverge og avdekke kriminalitet på en effektiv måte,

[90] Ot.prp. nr. 60 (2005-2005) Politidirektoratets uttalelse side 106

med hensynet til borgernes rettssikkerhet og personvern."[91] Når reglene nå har trådt i kraft, er det ikke tvilsomt at samfunnets interesse ble funnet å veie tyngre enn hensynet til den enkeltes personvern.

Som nevnt i 1.1 er bakgrunnen for de nye identifiseringshjemlene et høringsbrev sendt av Justisdepartementet i juni 2004. Forslaget ble fremsatt etter at politimetodeutvalget hadde levert sitt forslag, og det finnes derfor ikke mye forarbeider.[92] Av høringsinstansene var det kun Datatilsynet som mente reglene burde utredes grundigere før man åpnet for identifisering. Justiskomiteens flertall, alle unntatt representanten fra Sosialistisk Venstreparti (SV), gikk inn for vedtakelse av reglene.

I likhet med Datatilsynet og SVs representant, er jeg kritisk til masseavlyttingsreglene. Derimot mener jeg at identifiseringsmetoden i strpl. § 216 b er tilfredsstillende utarbeidet. Jeg er av den oppfatning at regelen burde vært utredet nærmere før den ble endelig vedtatt. Jeg ønsker selvfølgelig at alvorlige forbrytelser skal bli oppklart, og dersom det betyr at jeg må avlyttes er det greit. Når jeg likevel mener at reglene burde vært utredet nærmere, er det fordi jeg mener man ikke har fullstendig oversikt over konsekvensene av reglene. En vet eksempelvis ikke hvor mye samfunnet sparer ved at politiet nå kan iverksette kommunikasjonskontroll hurtigere.

Norge har tradisjonelt vært forsiktig med å benytte inngripende etterforskningsmetoder. Jeg er derfor av den oppfatning at en slik utvidelse av adgangen i bruken av tvangsmidler burde skje gradvis. En eventuell utvidelse bør skje på bakgrunn av de erfaringer man har gjort ved andre etterforskningsmetoder, eksempelvis identifisering etter strpl. § 216 b annet ledd litra c). Norge har tradisjonelt vært forsiktig med å benytte tvangsmidler i etterforskningsøyemed.

---

[91] Innst. O. nr. 113 (2004-2005) punkt 1.2

[92] Ot.prp. nr. 60 (2004-2005), Innst. O. nr. 113 (2004-2005) og Besl. O. nr. 100 (2004-2005)

Det er ikke tvil om at det finnes mange og gode rettssikkerhetsgarantier, men jeg er usikker på hvorvidt de foreliggende garantier er tilstrekkelige. Det er særlig inngripende for uskyldige tredjemenn som blir avlyttet i forbindelse med identifisering. Departementet og justiskomiteen forutsetter for eksempel at avlytting skal stoppes straks det er klart at vedkommende ikke har noe med saken eller mistenkte å gjøre. Det blir således forutsatt at misbruk ikke vil være et problem. Jeg er av den oppfatning at det alltid er fare for misbruk, selv om jeg helst vil tro at en polititjenestemann er lojal ovenfor sine arbeidsinstrukser. Det kan reises spørsmål om dette ikke kunne vært løst på en annen måte.

Det hersker også en del usikkerhet i forhold til manglende tidsbegrensninger. Det er forutsatt at identifiseringen ikke vil ta lang tid. Men dette vil nødvendigvis måtte avhenge av en del ytre momenter, eksempelvis vil en større bygning kreve mer ressurser enn et mindre område. Politiet er også avhengig av at mistenkte faktisk benytter kommunikasjonsanlegget. Dersom mistenkte ikke gjør det, vil avlyttingen ta lengre tid, og flere uskyldige vil da bli avlyttet. Dette er særlig aktuelt i forbindelse med den økende bruken av mobiltelefoner, som fører til at nordmenn i langt større grad fører samtaler hvor de enn ferdes. Dette vil muligens føre til at flere vil bli avlyttet i forbindelse med masseavlytting.

5 Kilder

5.1 Lovregister

5.1.1 Norske lover

1814 Kongeriget Norges Grundlov 17. mai 1814 (Grunnloven)

§ 96

§ 99

§ 110 c

1902 Almindelig borgerlig Straffelov (Straffeloven)

§ 44

§ 46

§ 49

§ 60 a

§ 61

§ 90

§ 91

§ 91 a

§ 94

§ 104 a

§ 144

§ 145 a

§ 162

§ 291

§ 317

§ 390 a

1967 Lov om behandlingsmåten i forvaltningssaker (Forvaltningsloven)

§ 4

1970 Lov om offentlighet i forvaltningen (Offentlighetsloven)

§ 6

1981 Lov om rettergangsmåten i straffesaker (Straffeprosessloven)

§ 4

§ 55

§ 61 a

§ 82

§ 92

§ 100 a

§ 170 a

§ 216 a

§ 216 b

§ 216 c

§ 216 d

§ 216 e

§ 216 f

§ 216 g

§ 216 h

§ 216 i

§ 216 j

§ 216 m

§ 222 d

§ 224

§ 381

1987 Lov om kontroll med eksport av strategiske varer, tjenester og teknologi m.v.

§ 5

1992 Lov om legemidler m.v. (Legemiddelloven)

§ 22

§ 24

§ 31

1995 Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste

§ 2

Lov om politiet (Politiloven)

§ 17 d

1999 Lov om (Menneskerettsloven)

§ 2

§ 3

2003 Lov om elektronisk kommunikasjon (Ekomloven)

§ 1-1

§ 2-9

5.1.2 Konvensjoner

Convention for the Protection of Human Rights and Fundamental Freedoms,

Roma 4. november 1950 (norsk tittel: Den europeiske menneskerettskonvensjon)

Artikkel 1

Artikkel 8

Vienna Convention on the Law of Treaties, Wien 23. mai 1969

(norsk tittel: Wienkonvensjonen)

Artikkel 4

Artikkel 31-33

5.1.3 Forskrifter

Forskrift om kommunikasjonskontroll (Kommunikasjonskontrollforskriften)

Fastsatt ved kgl. Res. Av 31. mars 1995 nr. 281, fremmet av Justis- og politidepartementet

§§ 2, 20-24

Forskrift om ordningen av påtalemyndigheten (Påtaleinstruksen) av 28. juni 1985 nr. 1679

§ 22-2

5.2 Forarbeider

5.2.1 Norges offentlige utredninger

NOU 1993: 18 Lovgivning om menneskerettigheter

NOU 1994: 4 Kontrollen med "de hemmelige tjenester"

NOU 1997: 15 Etterforskningsmetoder for bekjempelse av kriminalitet

NOU 2003: 18 Rikets sikkerhet

NOU 2004: 6 Mellom effektivitet og personvern – Politimetoder i forebyggende øyemed

5.2.2 Odelstingsproposisjoner

Ot.prp. nr. 10 (1976-77) Midlertidig lov om adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivning

Ot.prp. nr. 13 (1990-1991) Lov om endringer i midlertidig lov 17. desember 1979 nr. 99 om adgang til telefonkontroll ved etterforskning av overtredelser av narkotikalovgivning

Ot.prp. nr. 40 (1991-92) Om lov om endringer i straffeprosessloven (telefonavlytting i narkotikasaker)

Ot.prp. nr. 83 (1993-94) Om lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste

Ot.prp. nr. 31 (1997-1998) Endringer i lov om telekommunikasjon

Ot.prp. nr. 64 (1998-99) Om lov om endringer i straffeprosessloven og straffeloven m.v. (etterforskningsmetoder m.v.) (lov 3.desenber 1999 nr. 82)

Ot.prp. nr. 81 (1999-2000) Om lov om endringer i straffeloven og straffeprosessloven (bruken av varetektsfengsling mv.)

Ot.prp. nr. 58 (2002-2003) Om lov om elektronisk kommunikasjons (ekomloven)

Ot.prp. nr. 60 (2004-2005) Om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)

5.2.3 Innstilling til Odelstinget

Innst. O. nr. 113 (2004-2005) Innstilling fra justiskomiteen om lov om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)

5.2.4 Beslutning av Odelstinget

Besl. O. nr. 100 (2004-2005) Om endringer i straffeprosessloven og politiloven (romavlytting og bruk av tvangsmidler for å forhindre alvorlig kriminalitet)

5.3 Rettspraksis

5.3.1 Høyesterett

Rt. 1993 side 1302

Rt. 1995 side 18

Rt. 1999 side 1944

Rt. 2000 side 996

Rt. 2002 side 509

5.3.2 EMD

Case of Campbell v. the United Kingdom, A 233 (1992)

Case of Dudgeon v. the United Kingdom, A 45 (1981)

Case of Handyside v. the United Kingdom, A 24 (1976)

Case of Klass and others v. Germany, A 28 (1978)

Case of Kruslin v. France, A-176-A (1990)

Case of Lüdi v. Switzerland, A 238 (1992)

Case of Malone v. the United Kingdom, A 82 (1984)

Case of Niemitz v. Germany, A 251-B (1992)

Case of Olsson v. Sweden, A 130 (1988)

Case of Peck v. the United Kingdom, 36 EHRR 41 s. 719 (2003)

Case of PG and JH v. the United Kingdom, RJD 2001-IX s. 195 (2001)

Case of Silver v. the United Kingdom, A 61 (1983)

Case of Sunday Times v. the United Kingdom, A 30 (1979)

5.3.3 Den europeiske menneskerettighets Kommisjon

X v. Norway, 13564 (1988)

5.4 Litteraturliste

Andenæs, Johs. *Norsk straffeprosess* B. 2. 3. utg. Oslo: Universitetsforlaget, 2000. ISBN 82-00-45414-2

Bergh, Trond. *Overvåking i Norge 1914-1997 B. I, Overvåkingssystemet bygges opp 1914-1955*. Trond Bergh og Knut Einar Eriksen. Oslo: Cappelen akademisk forlag, 1998 ISBN 82-456-05875

Bernt, Jan Fridthjof. *Frihagens forvaltningsrett* B. 1. Jan Fridthjof Bernt og Ørnulf Rasmussen. 1. utg. Bergen: Fagbokforlaget, 2003. ISBN 82-7674-830-9,

Bjerke, Hans Kristian. *Enkelte spørsmål i tilknytning til telefonavlytting i narkotikasaker*. I: … den urett som ikke rammer deg selv Festskrift til Anders Bratholm 70 år. Oslo: Universitetsforlaget, 1990. Side 213 flg. ISBN 82-00-21011-1.

Bjerke, Hans Kristian. *Kapittel 16 A Avlytting og annen kontroll av kommunikasjonsanlegg (kommunikasjonskontroll)*. I: Straffeprosessloven kommentarutgave B. 1. Hans Kristian Bjerke og Erik Keiserud. 3.utg. Oslo: Universitetsforlaget, 2001. ISBN 82-15-00046-0

Eckhoff, Torstein. *Rettskildelære*. 5. utg. ved Jan Helgesen. Oslo: Universitetsforlaget, 2001. ISBN 82-518-3988-2

Eckhoff, Torstein. *Rettslige grunner for forvaltningens virksomhet. Legalitetsprinsippet m.v.* I: Forvaltningsrett. 7. utg. ved Eivind Smith. Oslo: Universitetsforlaget, 2003. ISBN 82-15-00397-4. Side [309-314]

Elden, John Christian. *Om personvern, avlytting og politistat*. I: Tidsskrift for Strafferett. Årgang 5 (2005) nr. 2. ISSN 1502 685X. Side 97-105

Elgesem, Frode. *Tolking av EMK – Menneskerettsdomstolens metode*. I: Lov og Rett. 2003 side 203

Eskeland, Ståle. *Forsøkshandlingen*. I: Strafferett. 1. utg. Oslo: Cappelen akademisk forlag, 2000. ISBN 82-02-19692-2. Side 203-214

Hov, Jo. *Prosessuelle grunnprinsipper og grunnleggende saksbehandlingsregler*. I: Rettergang I, Sivil- og straffeprosess. 1. utg. Oslo: Papinian AS, 1999. Kapittel 3. ISBN 82-91060-08-8. Side [75]-87

Hov, Jo. *Tvangsmidler, skjellig grunn til mistanke*. I: Rettergang II, Straffeprosess. Oslo: Papinian AS, 1999. ISBN 82-91060-09-6

Møse, Erik. *Menneskerettigheter*. Oslo: Cappelen akademisk forlag, 2002. ISBN 82-02-19801-1

Rognlien, Knut. *Advokater som gisler i telefonavlyttningssaker*. I: Tidsskrift for Strafferett. Årgang 4 (2004) nr. 1. ISSN 1502-685X. Side 81-87

Aall, Jørgen. *Første del: innledning, metode og rettskilder*. I: Rettergang og menneskerettigheter. Bergen Oslo: Universitetsforlaget, 1995. ISBN 82-00-22415-5. Side 9-88.

Aall, Jørgen. *Rettsstat og menneskerettigheter*. Bergen: Fagbokforlaget, 2004. ISBN 82-450-0209-7

5.5 Elektroniske dokumenter

Møse, Erik. *EMK art. 1*. I: Norsk lovkommentar. Oslo: Gyldendal. Note 1. Tilgang: www.gyldendal.no/rettsdata/

5.6 Rundskriv

Justisdepartementet, G-45/99 (1999)